UIC John Marshall Journal of Information Technology & Privacy Law

Volume 3
Issue 1 *Computer/Law Journal - 1981*

Article 9

1981

# Trade Secret Protection for Software Generally and in the Mass Market, 3 Computer L.J. 211 (1981)

Miles R. Gilburne

Ronald L. Johnston

# TRADE SECRET PROTECTION FOR SOFTWARE GENERALLY AND IN THE MASS MARKET†

*By* MILES R. GILBURNE & RONALD L. JOHNSTON*

TABLE OF CONTENTS





* Blanc, Gilburne, Peters, Williams & Johnston, 1900 Avenue of the Stars, Suite 1200, Los Angeles, California 90067.

The booming computer software industry has been and increasingly will be the source of controversy regarding issues of proprietary rights. The reasons for this phenomenon are several. While the software industry is new and rapidly expanding, older legal doctrine is not easily applied to its difficult technology and complex commercial relationships. Moreover, software development is creative and the industry is characterized by high employee mobility and relative ease of entry. At the same time, software duplication is relatively cost-free, and the determination of whether software was independently developed, or stolen, is often exceedingly difficult to make.

The legal ground rules that will govern the industry's development are very important to all of the participants. Employers must be wary of hiring programmers who may use trade secrets belonging to former employers. Employees must be wary of seriously diminishing their marketability because of covenants expressed in contracts or implied by law. Competitors must be wary of others obtaining their confidential information through former employees or access to documentation distributed on a limited basis. And end users and distributors must be wary of losing their source of supply, maintenance, and enhancements should their licensor be the subject of an action for trade secret misappropriation.

The trade secret laws offer one of the principal methods of protecting computer software. Unfortunately, it is often extremely difficult to determine what information is unique to a particular competitor—and thus should be protected from other competitors or use by an employee for his own benefit—and what information is generic to a profession or business and should not be so protected. Moreover, it is equally difficult in many cases to determine whether information has been the subject of independent development or has come into another's possession through misappropriation. Finally, with the emergence of new channels of distribution such as those designed to reach the mass market, the efficacy of trade secret protection for some software is very much an unknown. This article will address each of these subjects.

## I. APPLICABILITY OF TRADE SECRET LAW TO SOFTWARE

### A. Basic Definition of Trade Secret

Most states and all federal jurisdictions have approved all or part of the definition of "trade secret" set forth in section 757, com-

ment b, of the *Restatement of Torts* (the *Restatement*).[1] As defined by the *Restatement*, a trade secret may consist of:

> any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it.
>
> The subject matter of a trade secret must be secret . . . so that, except by the use of improper means, there would be difficulty in acquiring the information. An exact definition of a trade secret is not possible. Some factors to be considered in determining whether given information is one's trade secret are: (1) the extent to which the information is known outside of his business; (2) the extent to which it is known by employees and others involved in his business; (3) the extent of measures taken by him to guard the secrecy of the information; (4) the value of the information to him in developing the information; . . . (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.

The *Restatement* definition requires the presence of three elements as a condition to the existence of a trade secret: novelty, secrecy, and value in the trade or business of the putative trade secret owner.[2] These materials will deal mainly with the elements of secrecy and novelty. The element of value can usually be satisfied by use of the trade secret in a trade or business and these materials will generally assume the presence of such "value."

## B. Novelty in General

Computer-related trade secret cases have generally required the plaintiff to establish that the subject matter be, in some degree, original or novel and not generally or commonly known in the trade.[3] Thus, "matters of public knowledge or of general knowledge in [the] industry cannot be appropriated by one as his secret."[4]

Although there is authority for the literal proposition that "[a]n overwhelming majority of authorities on the subject have ruled that novelty and uniqueness are not a requirement for trade secret protection,"[5] courts granting trade secret protection typically find that the subject matter was "sufficiently novel."[6] At a minimum, it is clear that, in seeking trade secret protection, the plaintiff need not

---

1. Restatement of Torts § 757, comment b (1939); *see* R. Milgrim, Trade Secrets, ¶ 2.01 (1978) [hereinafter Milgrim].

2. Restatement of Torts § 757, comment b.

3. *See generally* Milgrim, *supra* note 1, at ¶¶ 2.01-.09.

4. Sperry Rand Corp. v. Pentronix, 311 F. Supp. 910, 913 (E.D. Pa. 1970).

5. Structural Dynamics Research Corp. v. Engineering Mechanics Research Corp., 401 F. Supp. 1102, 1117 (E.D. Mich. 1975).

6. *See, e.g.*, Data Gen. Corp. v. Digital Computer Controls, Inc., 357 A.2d 105, 110 (Del. 1975).

show that the subject matter possesses the same degree of novelty as is required for patent protection.[7]

### C. Novelty with Respect to Software

The qualities of software which most often qualify for protection as trade secrets are the elements comprising the software's unique logic and coherence. Three indicia of this unique logic and coherence are: (1) novel combinations of generally known concepts; (2) the dedication of time and expense to create features providing some competitive advantage, and (3) substantive uniqueness in application. Generic knowledge (i.e., knowledge generally known in the computer industry) is not subject to trade secret protection.

#### *1. Novel Combinations of Generally Known Concepts*

In *Com-Share, Inc. v. Computer Complex, Inc.*,[8] plaintiff developed a time-sharing operating system, together with a high-level programming language and text editor. After holding that this software was based upon "new principles and concepts with unique engineering, logic and coherence," the court dealt with defendant's claim that the software was not secret or new, but in the public domain:

> [T]he existing software systems which are unique in the computer time sharing industry all contain certain elements which perform similar functions and many utilize certain similar fundamental concepts, and in the most general sense, a common base. Such is common in all engineering. Thus, the concept of vehicular locomotion, involving in one aspect, the basic principles of the internal combustion engine, is common to snowmobiles, ships, airplanes, and automobiles. But there the similarity stops. The varying systems, as patent lawyers so eloquently demonstrate, differ greatly in the steps taken to accomplish the objective. Similarly here. The specific engineering of these software systems, and their particular underlying technologies and design, together with what has been referred to as their 'logic and coherence', as well as their speed, accuracy, cost and commercial feasibility, may differ greatly from system to system. They will and do inevitably reflect the peculiar and unique accomplishments and technical skills of the developers thereof. This, in a nutshell, is what the software systems developed by the plaintiff supplies to the defendant under the Technical Exchange Agreement. And while it is true that defendant may have made certain technical changes in software supplied to it by plaintiff under the Technical Exchange Agreement, the defendant did not alter the unique principles, engineering logic, and coherence de-

7. *See* Milgrim, *supra* note 1, at ¶ 2.08.
8. 338 F. Supp. 1229 (E.D. Mich. 1971).

veloped by plaintiff into such software system.[9]

The court in *Com-Share* correctly articulated one reason why most software will, assuming that its putative owner maintains the requisite level of secrecy, constitute a trade secret. For example, while the design of every inventory control or general ledger system will require the programming of similar algorithms and result in the production of functionally similar software, the multitude of specific programming decisions required as part of the development process will be made differently by different programmers and result in systems of different "speed, accuracy, cost and commercial feasibility." Thus, different software systems running on the same machine and processing the same data might exhibit different response times to user requests, different interface capabilities with other systems or different error detection techniques. Since the *Restatement* definition of a trade secret speaks in terms of "competitive advantage", trade secret protection should not be denied to software simply because it is developed through the use of generally known skills or the combination of generally known concepts. The "unique logic and coherence" produced by different applications of such skills or combinations of such concepts by individual programmers will produce a certain level of commercial feasibility which should constitute trade secret subject matter.[10]

With the exception of very simple programs involving few algorithms, none of which lends itself to multiple programming solutions, virtually all software will be the result of individual programming decisions made through the application of generally known programming skills or through the combination of generally known data processing concepts which in the aggregate, or in combination with each other, may rise to the level of a trade secret.

### *2. Dedication of Time and Expense*

Closely allied to the concept of "unique logic and coherence" and "commercial feasibility" as a basis for granting most software trade secret status is the fact that the development of a software

9. *Id.* at 1234.

10. *See, e.g.*, Cybertek Computer Products, Inc. v. Whitefield, 203 U.S.P.Q. (BNA) 1020 (1977) (defendant, who developed competing system similar to that of former employer, argued that former employer's Auto/Issue System could not constitute a trade secret insofar as it consisted of well-known concepts in the computer industry; the court held that, while general concepts are not protectable, the specific implementation of a particular combination of general concepts here constituted a protectable trade secret); Telex Corp. v. IBM Corp., 367 F. Supp. 258 (N.D. Okla. 1973), (in a hardware context, court held that features which in themselves were neither "new, novel, secret nor innovative" could in combination constitute a trade secret since they allowed IBM to "achieve its goals of the 38309 in terms of cost and performance").

system requires a great deal of time and effort. The employer who expends such time and effort to achieve a certain result has a competitive advantage over the competitor who has not expended such time and effort and therefore cannot achieve the same result. Such a competitive advantage should, under the definition set forth in the *Restatement*, be entitled to trade secret protection, despite the fact that it results simply from the dedicated application of generally known skills or combinations of generally known concepts. This conclusion is particularly important in an industry such as software development where technology moves at such a rapid pace that a small head start in reaching the market is often the difference between the economic success and failure of a given product.

This principle has been implicitly recognized by the courts. In fashioning injunctive relief for misappropriation of trade secrets, courts frequently have applied the "head start" doctrine which limits the length of injunctive relief for misappropriation of trade secrets to the time it would have taken the defendant to independently develop the trade secret.[11]

### *3. Substantive Uniqueness in Application*

The great majority of software-related trade secret cases which have been decided to date, and which are likely to be decided in the years to come, focus on software which is functionally similar to many competing systems that coexist in the marketplace and is therefore properly characterized as having been developed through the application of widely known skills or combination of generally known concepts. Several cases, most of which involve issues of patent protection, however, have been decided involving software which involves the application of data processing technology to functions not previously or commonly automated. Such software is obviously entitled to trade secret protection and, as discussed below, should perhaps be entitled to different treatment in the context of trade secret disputes than that accorded other types of software.[12]

---

11. *See* Winston Research Corp. v. Minnesota Mining & Mfg. Co., 350 F.2d 134, 142 (9th Cir. 1965); Analogic Corp. v. Data Translation, Inc., 358 N.E. 804, 807 (Mass. 1976).

12. See, for example, *In re* Diehr, 602 F.2d 982 (C.C.P.A. 1979), *aff'd sub nom.* Diamond v. Diehr, 450 U.S. 175 (1981) (patentability of method of using computer to control a rubber curing process); *In re* Bernhardt, 417 F.2d 1395 (C.C.P.A. 1970) (patentability of method of using computer to illustrate 3-Dimensional object); Parker v. Flook, 437 U.S. 584 (1978) (patentability of method for developing update parameters to detect the presence of abnormal conditions in catalytic conversion); Structural Dynamics Research Corp. v. Engineering Mechanics Research Corp., 401 F. Supp. 1102 (E.D. Mich. 1975) (employer/employee trade secret dispute involving software developed to utilize isoparametric elements in structural analysis).

*4. Generic Versus Specific in the Employment Context*

While no item can be accorded trade secret protection unless it possesses a certain element of novelty, the public policy against post-employment restrictions often causes a trade secret plaintiff to face more difficulty in establishing the requisite element of novelty than if the misappropriation had taken place outside the context of an employer/employee relationship. The reason for such additional burden is the difficulty in determining whether or not items which an employer seeks to bring within the umbrella of trade secret protection are in fact knowledge generically necessary to the practice by an employee of his chosen business in a given industry or generally known to those familiar with such industry. To the extent that knowledge is viewed as generically necessary or as generally known information, it is not protectable as a trade secret.[13] A review of case law on this issue permits generalization of some analytical distinctions which will now be examined.

*a. Knowledge Gained About Particular Vertical Markets*

Although much similarity exists among software systems designed to perform similar functions (e.g., inventory control or general ledger) in different types of business (e.g., home improvement centers or supermarkets), knowledge of the specific needs of a given type of business (commonly referred to as a "vertical market") is an invaluable aid in designing a system for that business. It has been held that the knowledge of a particular vertical market gained by an employee in the design of a system for that vertical market is general information which such employee should be able to use in developing a competing system.

For example, in *Automated Systems, Inc. v. Service Bureau Corp.*,[14] plaintiff developed inventory control software for the automotive parts business in which data base updating was made through punch cards kept in a "tub file." Defendant, after contracting to act as the exclusive sales agent in marketing the plaintiff's inventory control system on a trial basis, terminated its contract with plaintiff after the trial period expired and developed a similar, competing system where input was made through tape from an adding machine. The employee most responsible for developing defendant's inventory control system, had, prior to beginning the

13. Telex Corp. v. IBM Corp., 510 F.2d 894, 929 (5th Cir. 1975) (employee cannot be restrained from using or disclosing to subsequent employers "information acquired during the course of previous employment which was a matter of general knowledge" or was "general technical or business information learned in former employment"); MILGRIM, *supra* note 1, at ¶ 5.02.

14. 401 F.2d 619 (10th Cir. 1968).

trial period in the exclusive sales contract, wide experience in data processing and systems analysis, but had gained all of his expertise in the automotive parts business while working with plaintiff under the exclusive sales contract. The court held that the knowledge about the automotive parts business which the employee gained from his dealings with plaintiff during the trial period was merely "general information" about that type of business not entitled to trade secret protection.[15]

### b. *Knowledge Which Employee Would Have Gained in Comparable Employment With a Different Employer*

Although the learning curve for the less skilled may be steeper than that for the more experienced, every software programmer will increase his skills and knowledge with each task that he completes. This phenomenon is obviously not limited to the software industry and, in fact, the promise of increased training (and corresponding increase in marketability) in one's profession by exposure to unfamiliar areas is frequently a prime motivation for selecting one potential employer over another. The mere fact that an employer provides training in a particular aspect of an industry is not sufficient to allow that employer to prevent his employees from utilizing what they learn in the course of that training for their own or a subsequent employer's benefit if the employee would have learned such information in the course of similar employment elsewhere.

Reduced to its fundamentals, this principle is a restatement of the basic tenet of trade secret law requiring novelty as a condition to legal protection. Where an employee could have gained comparable training elsewhere, the balancing of an employer's need for trade secret protection against the public policy encouraging employee mobility strongly suggests a finding of non-infringement.[16]

---

15. *Id.* at 609. *See also* Trilog Assoc., Inc. v. Famularo, 455 Pa. 243, 314 A.2d 287 (1974) (former employee had only learned general, not confidential, information about certain aspects of banking business in the course of developing certain banking software).

16. *See* Wilson Certified Food, Inc. v. Fairbury Food Prods., Inc., 370 F. Supp. 108 (D. Neb. 1974) (plaintiff's employee developed process for creating bacon bits in the course of his employment with plaintiff and, upon a finding that such process was widely known in the food industry, trade secret protection was denied); Berkshire Apparel Corp. v. Stogel, 360 Mass. 863, 277 N.E.2d 310 (1971) (employer's general knowledge and experience in its industry could not be claimed a trade secret so as to prevent employee from continuing to work in same industry); MILGRIM, *supra* note 1, at ¶ 5.02.

### D. SECRECY WITH RESPECT TO SOFTWARE

The *Restatement* definition and numerous cases establish that the existence of a trade secret depends upon the subject matter for which protection is sought remaining "secret."[17]

#### *1. In-House Measure to Protect Secrecy*

##### *a. Case Example*

In *Telex Corp. v. IBM Corp.*,[18] evidence showed that IBM had its employees sign an "Employee Confidential Information and Invention Agreement" at the commencement of their employment with IBM and, at least as to the employees that were subsequently hired by IBM's competitor, Telex, that IBM had reminded them prior to their departure that they had had access to proprietary, confidential and trade secret information and were contractually prohibited from disclosing this information to others. In addition, IBM used magnetic locks on building doors to allow access only to authorized personnel, as well as document control procedures, guards, television cameras, sensors, locks, safes and computer-controlled access systems; it even manufactured sensitive hardware components in-house rather than having them contracted to outside vendors. The trial court not only found that IBM had taken sufficient precautions to protect its secrets, but assigned part of the cost of those measures as damages attributable to Telex's unlawful attempt to penetrate the secrets.[19] The Tenth Circuit, while agreeing that IBM's security measures were sufficient, disallowed the damage award with respect to the cost of such measures to IBM for lack of proximate cause.[20]

---

17. *See* MILGRIM, *supra* note 1, at ¶ 2.03. The following discussion is intended to provide a relatively comprehensive list of "secrecy" measures which, in an ideal world, might be adopted by a company desiring to protect its information or a trade secret. Many of these measures will simply be impractical for companies to adopt given the day to day realities of their businesses. Fortunately for trade secret plaintiffs, only "relative" rather than "absolute" secrecy is required for maintenance of a trade secret. See *infra* note 32 and accompanying text.

18. 367 F. Supp. 258 (N.D. Okla. 1973).

19. *Id.* at 330.

20. Telex Corp. v. IBM Corp., 510 F.2d 894 (10th Cir. 1975). *See also* Structural Dynamics Research Corp. v. Engineering Mechanics Research Corp., 401 F. Supp. 1102, 1117 (E.D. Mich. 1975) ("Although [the employer] did not use the ultimate in policing measures, the professional caliber of its employees, and true nature of its development work [in software support for structural analysis programs] made heavy-handed measures unnecessary"); Digital Dev. Corp. v. International Memory Sys., 185 U.S.P.Q. (BNA) 136 (S.D. Cal. 1973) (trade secret in disc memory; no express non-disclosure agreement necessary where employee actually knows that information is trade secret; non-secret manufacturing conduct at the plant did not destroy trade secret elements of the product); Com-Share, Inc. v. Computer Complex, Inc., 338 F. Supp. 1229 (E.D. Mich. 1971) (hardware and software; plaintiff used "utmost caution"

*b. Physical Control of Premises*

Access to any sensitive areas should be restricted to approved personnel. I.D. badges or sign-in/sign-out procedures may facilitate the control of access. Devices to detect intruders may be advisable.

Sensitive areas should be locked securely and premises may be divided and compartmentalized to control the flow of sensitive materials. Limiting the number of doors and windows in sensitive areas will decrease the threat of break-in. In addition, attention should be directed to possible avenues of access to restricted areas through stairways, roofs, mail slots, basements and adjoining buildings. Security guards may be needed.

Terminals or other peripheral devices through which important materials may be accessed should be in secure locations accessible only to authorized personnel. Keys, combinations or passwords may be required to operate certain equipment or to access certain files. Other more exotic procedures such as voiceprint identification devices or devices that identify fingerprints or hand geometry may also be considered. Keys to doors and terminals, combinations, passwords and similar security devices should be changed regularly, and also should be changed whenever an employee with access to such a key or code leaves the organization, and whenever it becomes apparent that security has been compromised.

Access to any tape library should be restricted carefully. It should be required that all tapes be signed in and signed out at all times.

All trash, scratch pads, tapes, residual data, notes, and similar materials should be disposed of in a manner that assures that no useful information can be obtained from them. Trash containers often are one of the most fruitful sources for those seeking access to confidential information. If a shredder or similar device is purchased, it should be able to accomodate all the different kinds of materials that may need to be destroyed.

*c. Establishing an Employee Trade Secret Program*

All employees and other parties having access to any proprietary materials should be required to sign a confidentiality and nondisclosure agreement. Ideally such agreements should be executed

---

in protecting its trade secrets where each page of listings embodying plaintiff's systems contained the words "Com-Share, Inc. Company Confidential"; where "passwords" were built into the system to prevent unauthorized access; and where tapes were kept locked when not in use); Sperry Rand Corp. v. Pentronix, Inc., 311 F. Supp. 910 (E.D. Pa. 1970) (magnetic memory cores; trade secrecy preserved where employees had signed non-disclosure agreement).

at the outset of employment. If such a confidentiality and non-disclosure agreement is executed after commencement of employment, any restrictive covenants may not be binding unless there is "new" consideration. Continuation of employment at will generally is not sufficient consideration to justify enforcement of a restrictive covenant.[21] If supported by the actual facts, it may therefore be advisable to provide in such agreement with already existing employees that the agreement simply confirms already existing policies known to the employees at the time of first employment. Some "new" consideration might be introduced, e.g., a change in benefits or profit sharing, or a firm commitment to retain the employee for some fixed period of time.

Whenever personnel leave their employment, a session should be held during which the employee is reminded of his or her obligations to maintain the organization's trade secrets. A termination agreement should also be executed by the employee acknowledging such restrictions. The refusal of an employee to sign such an agreement could give rise to an inference that the employee intended to misappropriate secrets (otherwise he or she would not have been reluctant to acknowledge the secrecy obligations).[22]

All personnel should be instructed as to the importance of security and the steps being taken to preserve secrecy. Procedures should be established and personnel should be instructed on how to proceed in the event of certain breaches of security, e.g., how to respond to the presence of unauthorized personnel in a secure area. Procedures also should be established for securing the building at night and prior to any evacuation of the building due to fires or bomb threats. Fires may be started or bomb threats instigated by personnel within the organization, and the confusion of evacuation may present an ideal opportunity for normal security procedures to be ignored and for materials to disappear.

Notice should be displayed prominently on walls and bulletin boards reminding employees of the confidential nature of their work and the importance of preserving secrecy.

Consideration should be given to designating certain specific materials as "SECRET AND CONFIDENTIAL" or "FOR INTERNAL USE ONLY" or similar designation. Such notices may, however, serve to pinpoint precisely which materials are most sensitive and thus direct a thief to the most valuable documents. Particular individuals within the organization should be assigned responsibility for the security program. If any procedures or policies are breached by

21. *See* Kadis v. Britt, 224 N.C. 154, 29 S.E.2d 543, 548 (1944).

22. An overreaching exit form will, however, provide the employee with an obvious justification for refusing to sign.

any employees, disciplinary measures should be taken to convey to all employees that such behavior will not be tolerated. Senior management should adhere to the same policies and procedures as other employees in order to emphasize the significance of protecting trade secrets and the organization's commitment to that goal.

Any employee who is terminated or who may be disgruntled should be immediately excluded from access to sensitive areas and materials, and all other employees should be immediately notified of such action. Personnel should be instructed not to leave sensitive materials lying in plain sight on desks and work tables. Access to copying machines should be restricted, particularly outside of normal working hours.

Various safeguards can be built into a computer system containing sensitive information. Access to certain files can be restricted to those who have a "need to know." Audit trails, transaction logs, and similar measures can be implemented to deter unauthorized access and to help pinpoint possible breaches of security after they have occurred.

Communication lines should be protected against wiretaps. Cryptographic devices may be used to scramble signals, and one can make it physically difficult to tap the lines. Wiretapping is, contrary to common belief, most likely to occur on the same premises as the hardware. Limiting access to the few places in the building where communications circuits are sufficiently well labeled for someone to know which line to tap (e.g. a communications circuit box) will eliminate the easiest way to tap the lines.

Periodic reviews of the secrecy program with input from all segments of the organization is essential. Additionally, speeches and outlines prepared by employees should be reviewed from time to time to be certain trade secrets are not being revealed.

### *2. Preserving Secrecy in Distribution of Software*

#### *a. General*

Internal measures aimed at protecting the secrecy of a claimed trade secret must, if the trade secret is to be maintained, be coupled with efforts to protect secrecy in the course of distribution to customers. These efforts generally take the form of restrictions imposed on customers with respect to the use, duplication and disclosure of the trade secret. It is critical to bear in mind that once a trade secret is placed in the public domain either by reason of inadequate internal controls or by reason of unrestricted dissemination to the public in the course of marketing, the trade secret is lost for all purposes.

*b. Use of License Rather than Sale Agreements*

It is generally thought that the license rather than the sale of software is more consistent with the retention of trade secret rights in such software. It is conceptually meaningful to retain proprietary rights in and title to a licensed product, while it is conceptually inconsistent with a sale to retain such right and title in a product which is sold.[23] Moreover, under both antitrust principles and in light of policies against restraints on alienation, the necessary restrictions on use or disclosure of a licensed product are more likely to be enforceable than with respect to a product that is sold.

*c. Typical Restraints Imposed on Customers Receiving Copies of Software*

The following restraints are commonly found in software license agreements relating to the use and disclosure of the software:

(i) Prohibition on copying other than for archival or back-up purposes;

(ii) No disclosure except to the customer's employees in the course of their employment as necessary to utilize the software;

(iii) Requirement that employees of the customer receiving access to the software sign confidentiality agreements directly enforceable by licensor;

(iv) Limitation of use to single central processing unit ("CPU");

(v) Restriction on processing of third party data;

(vi) Requirement that the customer notify licensor of unauthorized use or disclosure, and requirement that the customer take legal action against third party who gains access to software and is using it on an unauthorized basis as a result of the customer having failed to comply with the contractual restriction; and

(vii) Requirement that distributors of software obtain license agreements from their customers containing nondisclosure restriction.

*d. Practical Methods for Preserving Trade Secrecy and Detecting Misappropriation of Computer Software*

A number of practical methods have been developed which may support an argument that the trade secrets contained in software can be kept out of the public domain despite a vigorous marketing

23. *Cf.* Section II *infra* for a discussion of the feasibility of retaining trade secret protection in a sold item in circumstances where the trade secrets embodied in such item are not readily ascertainable upon inspection.

effort. These methods are generally used in conjunction with license restrictions, although Section II below will examine whether such methods might, standing alone, be sufficient to protect the secrecy of the trade secrets in software. Because of the difficulty in proving trade secret misappropriation (see discussion in Section IV below), these methods are particularly significant since they may, as a practical rather than legal matter, hinder the misappropriation of the trade secrets. The following methods may also be used to assist in the detection of misappropriation.

(i) Programs or data files can be stored only in encrypted or enciphered form, thus rendering them unintelligible unless deciphered.

(ii) Firmware such as read-only memory ("ROMs") may be mounted in a cassette or on a circuit board and covered with an opaque resin or epoxy which is difficult to remove without damaging the firmware.

(iii) A program may be distributed in more than one medium, all of which are essential for the program to execute. For example, the majority of a program may be on a floppy disk, with small but critical portions (e.g., a cipher key) contained on a ROM which either is an integral part of the hardware or must be connected to a circuit board by the end-user.

(iv) Hardware may be designed so that many programs are integrated into the hardware configuration on firmware, but can only be activated by authorized service personnel.

(v) Hardware and software can be designed to be incompatible unless a particular copy of the software is run on a particular machine. This may be a useful technique to use for operating systems software, though it may raise antitrust issues.

(vi) Various elements can be embedded in a program to facilitate proof that copying has occurred, e.g. duplicative runaway logic, dead code, unexecutable code, copyright or other proprietary rights notices, or other identifying materials.[24]

(vii) A program can be designed with certain "time-fuses" so that it will not execute unless periodically updated or serviced by authorized personnel. Creative programmers can also build safeguards into a program which causes it to ignore an instruction to

24. *See* Williams Elec. v. Arctic Int'l, Inc., Civil Action No. 81-1852 (D.N.J. 1981) (program allegedly duplicated by defendant from plaintiff's program for an electronic coin-operated game contained an identical error, sets of initials and high scores of several of plaintiff's employees involved in the original testing of the program including plaintiff's president, and copyright notices in plaintiff's name which were stored within the program so that the notice would not normally be displayed on the CRT while utilizing the program).

"dump" or print-out its entire contents, to erase critical portions of itself, to shut down the main CPU, to leave clear signals that a breach of security has occurred, and other similar protective mechanisms.

(viii) Serial numbers or similar unique identifying elements can be embedded in programs to aid in pinpointing the source of any unauthorized duplication.

(ix) The program may be distributed only in machine-readable object code, as distinguished from human understandable source code. With the increasing availability and sophistication of "decompliers" and "disassemblers" which can (to varying degrees) reverse object code into source code, the efficacy of object code dissemination exclusively as a method of protecting the trade secrets contained in a particular software program is somewhat diminished. See Section II below for a discussion of the impact of decompilation and disassembly on the ability to protect software in the mass market.

(x) Blank tracks can be included on floppy discs containing software.

(xi) Nonstandard markets, trailers and checksums can be used to delimit address and data fields.

(xii) Data can be recorded midway between normal track positions.

## II. SPECIAL PROBLEMS OF PROTECTING THE TRADE SECRET NATURE OF SOFTWARE IN THE MASS MARKET

### A. The Issues

With the advent of relatively low cost microprocessor-based hardware and the massive increase in the number of such computers now being sold, the software industry has become increasingly focused on the production of mass-distributed software for use on the "personal" or "small business" machine. This software is (i) generally written in a very high level language, (ii) distributed at a very low per copy cost, (iii) often marketed by mail order or through retail stores and (iv) if successful, distributed to thousands of users.

A number of significant trade secret issues are raised by the mass-distribution of microprocessor software:

1. Is it practical for software developers to obtain signed nondisclosure agreements from thousands of users, many of whom will be using such software in their homes and may be intimidated by a formal license agreement? This issue becomes particularly signifi-

cant in a mail order context when customers simply send in a check for $100 and expect to receive a copy of the software by return mail.

2. Even if license agreements are obtained from customers, will the circumstances under which such agreements are generally obtained affect the enforceability of such agreements in the courts?

3. Even if enforceable license agreements are obtained from all customers, does the fact that many thousands of copies of the software are distributed nonetheless mean that the software cannot reasonably be viewed as "secret"? Such a conclusion might result in the loss of trade secret protection for such mass-distributed software.

4. Given the practical difficulties of obtaining license agreements from customers acquiring mass-distributed software, it is likely that some percentage of such customers will not be party to a formal license agreement. Does such a percentage failure cause the developer to lose trade secret protection?

5. Does the existence of practical protections for mass-distributed software as described in Section I above provide the developer of mass-distributed software with a means of retaining trade secret protection for such software despite wide distribution and imperfect or nonexistent licensing practices?

### B. Obtaining the License Agreement

In recognition of the tremendous administrative and practical difficulties of obtaining executed license agreements from customers of mass-distributed software, developers have increasingly been abandoning such an approach. Instead, licensors are simply providing the software in a sealed diskette and are, concurrent with the delivery, providing the customer with a set of Standard License Terms and Conditions. These terms and conditions, as well as a legend placed on the diskette, specify that the customer will be deemed to have accepted the Standard License Terms and Conditions by the act of breaking the seal on the diskette or actually using the software. In a mail order context, licensors are providing that if the customer does not want to accept the terms and conditions of license, he can simply return the unopened diskette to the licensor and receive a full refund of monies paid.

Another approach taken by licensors is to condition a warranty or right to receive updates or notice of updates upon return of a signed warranty card which also includes an acknowledgment and acceptance of the terms and conditions of license.

### C. Enforceability of License Agreements for Mass Distributed Software

It is likely that license agreements with end-users obtained in a manner similar to that described above will be subject to attack using familiar consumer-oriented arguments such as adhesion and unconscionability. Licensors should be able to argue that software users are sufficiently sophisticated to understand the nature of and need for a simple commitment of non-duplication. Obviously, this argument will be the liveliest with respect to the true home users of personal computers. It is interesting to speculate on the impact that a court opinion voiding such an agreement with respect to a particular software product would have on trade secret protection claimed by licensors of other mass distributed software. If courts begin to view such agreements as unenforceable, can a licensor of mass-distributed software reasonably rely on such agreements as a basis for maintaining the "secret" nature of their software?

### D. Impact of Mass Distribution on Secrecy

Even if enforceable license agreements are obtained from all end-users of mass-distributed software, an issue still exists as to whether or not the mere fact of massive distribution is inconsistent with the "secrecy" element of trade secret protection.

#### *1. Case Law*

It is clear that disclosure of trade secrets in the course of a confidential relationship (either implied by law or created by contract) does not cause the trade secret to cease being "secret" for purposes of trade secret law. Although the issue has not been specifically decided for mass-distributed software, relevant case authority suggests that the number of copies distributed in confidence should not, as a matter of law, result in the loss of trade secret protection for the information embodied in such copies.

##### *a. Board of Trade v. Christie*[25]

The Chicago Board of Trade sought to prevent the use and distribution, by the defendants, of the continuous quotations of prices on sales of grain futures which the Board collected and confidentially communicated to a great number of its own customers. In affirming the judgment for the Board, the Supreme Court stated:

> In the first place, apart from special objections, the plaintiff's collection of quotations is entitled to the protection of the law. It

25. 198 U.S. 236 (1905).

> stands like a trade secret. The plaintiff has the right to keep the work which it has done, or paid for doing, to itself. The fact that others might do similar work, if they might, does not authorize them to steal the plaintiff's.[26] The plaintiff does not lose its rights by communicating the results to persons, even if many, in confidential relations to itself under a contract not to make it public, and strangers to the trust will be restrained from getting at the knowledge by inducing a breach of trust, and using knowledge obtained by such a breach.[27]

*b. Pressed Steel Car Co. v. Standard Steel Car Co.*[28]

In this case, plaintiff distributed railroad car designs to purchasers for limited purposes which the court found were understood by such purchasers despite the absence of express contractual restrictions. Despite evidence indicating that distribution of the design drawings was "so great that an investigation at trial of the circumstances of each was a practical impossibility," the court held that such broad disclosure could not defeat a claim for trade secret protection in the design drawings when such disclosure was made on a restricted basis.[29]

*c. Data General Corp. v. Digital Computer Controls, Inc.*[30]

In this case, plaintiff Data General sought trade secret protection for maintenance diagrams which, according to defendant's claims, were accessible by almost 6,000 people by the time of trial. The court found that Data General had taken adequate measures to protect the confidentiality of the diagrams, stating that "dissemination is not significant if in confidence."[31]

*2. Relative Versus Absolute Secrecy*

The ability to maintain trade secret protection for mass-distributed software may ultimately turn on application of the well-established principle that relative or qualified, as opposed to absolute, secrecy is all that is required by trade secret law.[32]

For example, in *K-2 Ski Co. v. Head Ski Co.*,[33] the Ninth Circuit held that:

---

26. *Cf.* Bleistein v. Donaldson Lithgraphing Co., 188 U.S. 239 (1903).
27. *Id.* at 250-51 (emphasis added).
28. 210 Pa. 464, 60 A. 4 (1904).
29. *Id.* at 468, 60 A. at 8.
30. 357 A.2d 105 (Del. Ch. 1975).
31. *Id.* at 114.
32. Data Gen. Corp. v. Digital Computer Controls, Inc., 297 A.2d 436, 438 (Del. 1972).
33. 506 F.2d 471 (9th Cir. 1974).

> There are two common law doctrines on secrecy: (1) absolute secrecy and (2) relative secrecy. The better view . . . is the majority view of relative secrecy which has been adopted by the Restatement of Torts § 757 . . . and that reasonable measures under the circumstances be taken to protect the secret . . . . The necessary determination of '[w]hether such a degree of secrecy existed in a particular case is a question of fact[;]' . . . and the trier of fact must consider 'the entirety of circumstances surrounding use' of the secret . . . .[34]

As the court in *K-2 Ski* recognizes, the question of secrecy is one of fact to be analyzed in view of all of the surrounding circumstances. It is likely that courts will find the mass distribution of software to thousands of users (even if accompanied by confidentiality legends or license agreements) relevant to such a factual inquiry. Courts should not, however, hold that such mass-distribution will, as a matter of law, defeat a claim for trade secret protection.[35]

Presumably, the potential non-enforceability of license agreements with consumers, as well as a licensor's expectation that not all licensees will sign or agree to such license agreements prior to receipt of the software, will also be thrown into the mix of facts relevant to the determination of "qualified secrecy."

Finally, the mere affixation of a copyright notice on software should not, as a matter of law, defeat a claim for trade secret protection, although such affixation may be factually relevant to a determination of whether or not sufficient security measures have been adopted.[36]

### *3. Relative Secrecy and Practical Protections for Mass Distributed Software*

Since it can be assumed that all or some copies of most mass-marketed software will, either intentionally or otherwise, be distributed to end-users without the protection of license agreements, the issue arises as to whether or not such unprotected disclosure will cause the developer to lose trade secret protection for the software.

#### *a. General Principles*

Courts have unanimously approved of the proposition that un-

---

34. *Id.* at 473-74.

35. *See* Management Science Am., Inc. v. Cyborg Sys., Inc., 6 Computer L. Serv. Rep. (Callaghan) 921 (N.D. Ill. 1978).

36. *See* Warrington Assoc., Inc. v. Real Time Eng'g Sys., Inc., 522 F. Supp. 367 (N.D. Ill. 1981); MILGRIM, *supra* note 1, at ¶ 2.06A(2)(6).

protected disclosures of secrets forfeit trade secret protection.[37] When a product is marketed on an unrestricted basis, and the product has a "secret" associated with it, the secret will be lost if it can be discerned upon scrutiny and inspection.[38]

It is also well established that trade secret protection may be lost through the type of disclosure occurring in advertising, circulars passed around in the trade, or in other analogous manners.[39]

In *Wheelabrator Corp. v. Fogle*,[40] the court held that the publication of a photograph of allegedly secret heat treating equipment in the annual report of the company constituted unprotected disclosure, even though the report was not itself addressed to a technical audience. The court, noting that scrutiny by experts divulged substantial aspects of the alleged secret, indicated that the company's cavalier publication of such photographs demonstrated a lack of "secretive intent" on the part of the company. The court held in that circumstance the trade secret protection was lost.

Courts have even held that disclosures in technical publications of very general aspects of a trade secret will result in the loss of trade secret protection if the disclosure enables one skilled in the art to discern the subject matter.[41]

Some courts have also found that use or release of information within the scope of claimed trade secrets, by individuals other than the party claiming ownership of a trade secret, can undermine the secrecy status of the trade secret, thereby undermining any claims which such a party might have.[42]

---

37. *See* Sinclair v. Aquarius Elec., Inc., 42 Cal. App. 3d 216, 116 Cal. Rptr. 654 (1974).

38. *See* Futurecraft Corp. v. Clary Corp., 205 Cal. App. 2d 279, 23 Cal. Rptr. 198 (1962); National Welding Equip. Co. v. Hammond Equip. Co., 165 F. Supp. 788, 795 (N.D. Cal. 1958); Speedry Chem. Prods., Inc. v. Carter's Ink Co., 306 F.2d 328, 334 (2d Cir. 1962).

39. *See* Republic Sys. & Programming, Inc. v. Computer Assistance, Inc., 322 F. Supp. 619, 628 (D. Conn. 1970) (plaintiff's advertising brochures listing the names of customers for computer programming services was held to preclude a claim of trade secret); Midland-Ross Corp. v. Sunbeam Equip. Corp., 316 F. Supp. 171 (W.D. Pa.), *aff'd per curiam*, 435 F.2d 159 (3rd Cir. 1970) (operating instructions provided to customers held to disclose the trade secret); Hahn & Clay v. A.O. Smith Corp., 320 F.2d 166 (5th Cir. 1963) (held that disclosure occurred through advertising brochures and technical papers delivered to trade and professional groups).

40. 438 F.2d 1226 (5th Cir. 1971).

41. *See* Struthers Scientific & Int'l Corp. v. Rappl & Hoenig Co., 453 F.2d 250, 254-55 (2d Cir. 1972).

42. *See* Future Plastics, Inc. v. Ware Shoals Plastics, Inc., 340 F. Supp. 1376 (D.S.C. 1972).

*b. Retention of Trade Secret Protection Despite Disclosure Without Restriction on Use: The Issue of Reverse Engineering*

The foregoing principles relating to loss of trade secrecy upon unprotected disclosure do not specifically address what is perhaps the most critical issue in mass-distributed software: Do trade secrets embodied in mass-distributed software marketed without restrictions on further disclosure retain their trade secret status if they cannot be readily ascertained from the copies of the software actually distributed? An analysis of this issue requires an understanding of the status of reverse engineering under trade secret doctrine.

Reverse engineering is the process by which a product is examined and analyzed in order to reveal the process by which it was created.[43] Trade secret law does not prevent someone who obtains a product on the open market or through other permissible means from using reverse engineering to discover the "secret" of a product and thereafter to use such "secret."[44] Of course it is possible that such reverse engineering may still infringe upon a patent or copyright or may result in a violation of trademark protection.

While it is clear that someone who actually does reverse engineer a product is free to do so, a more difficult question is whether the fact that a product can be reverse engineered deprives the owner of the "secrets" contained therein of trade secret protection as against a potential defendant who obtains the "secrets" by other means, such as through a confidential relationship or through outright theft. Although there is language in many cases which implies that there is no trade secret protection in such an instance because there is no "secret," the facts of such cases generally reveal that (i) defendant actually did "reverse engineer the product" or (ii) the so-called secret was so readily ascertainable from an inspection of the product that very little time or effort would be necessary in order to duplicate the product or secret.[45]

The issue of trade secret protection for ideas embodied in products distributed widely without restriction on use or disclosure would thus seem to turn on how difficult it is to "reverse engineer" the product. This concept is supported by comment B to the *Restatement* definition of a trade secret where it is indicated that one

43. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974).

44. Analogic Corp. v. Data Translation, Inc., 358 N.E.2d 804, 807 (Mass. 1976) ("a device which has been described in trade journals and placed on the market is generally open to duplication by skilled engineers"); *see generally* MILGRIM, *supra* note 1, at ¶ 2.05[2] and cases cited therein.

45. *See generally* cases cited in MILGRIM, *supra* note 1, at ¶ 2.05[2] & n.8.

of the factors in determining whether a trade secret exists is "the ease or difficulty with which the information could be properly acquired or duplicated by others."[46] This concept is consistent with the idea that a trade secret is in fact something which gives its owner a "competitive advantage" over others. Accordingly, if it will take competitors an extensive period of time and require the expenditure of significant funds to duplicate the "secrets" in a product on the open market, manufacturers of such a product should be viewed as having a trade secret to the extent of this time and cost advantage. There is in fact extensive case authority to the effect that this is a correct statement of the law.[47]

A more recent case reflecting this principle of trade secret law is *Colony Corp. of America v. Crown Glass*,[48] in which the court stated:

> Where a product is out on the market, and the secret is readily disclosed by the product itself there is no trade secret . . . . If the secret is not easily ascertainable from the product itself, however, the sale of the products may be enjoined in order to protect the secret despite the fact that the products are not themselves trade secrets but are only the fruits of the use of a trade secret . . . . The injunction in such a case is limited in scope to the time interval required for another to copy legally the secret from the goods on the market. . . .[49]

### c. *Effect of Possibility of Reverse Engineering on Scope of Relief*

Even if reverse engineering of a product or process is sufficiently difficult to justify a conclusion that the manufacturer of a product marketed on an unrestricted basis has a valuable advantage

---

46. RESTATEMENT OF TORTS, § 757, *supra* note 1, at comment b.

47. *See, e.g.*, Thermotics, Inc. v. Bat-Jac Tool Co., 541 S.W.2d 255, 260-61 (Tex. Civ. App. 1976) (where the court contrasted ideas which were "readily ascertainable" by inspecting and reverse engineering and therefore not protectible as trade secrets, with more complex ideas not readily discernable which were held protectible despite the fact that they may have been technically disclosed or ascertainable); *cf.* A.F. Holden Co. v. O'Brien, 73 U.S.P.Q. (BNA) 481 (E.D. Pa. 1947) (no trade secret if formula is readily ascertained through analysis by others in the trade). *See also* Clark v. Bunker, 453 F.2d 1006, 1010 (9th Cir. 1972) (appropriation of plaintiff's business plans and methods actionable despite the fact that such plans and methods could have been independently ascertained due to difficulty and cost of doing so). *See generally* MILGRIM, *supra* note 1, at ¶ 2.03 and cases cited in n.12; *see also* Maruchinics, *Industrial Trade Secrets: Their Use and Protection*, CLEV.-MAR. L. REV. 69-71, 72 (1975).

48. PAT. TRADEMARK & COPYRIGHT J. (BNA), Jan. 21, 1982, at A-13 (Ill. App. Ct. Dec. 16, 1981).

49. *Id.* at A-14.

over its competitors, the possibility of reverse engineering may nevertheless lead to a limitation on the extent of the protection which will be available to such manufacturers under trade secret principles.[50]

The fact that a product can be reverse engineered suggests that injunctive relief for misappropriation of trade secrets contained in such product should be limited to the length of time it would take for someone independently to develop or reverse engineer the secret by permissible methods. This principle is sometimes referred to as giving a trade secret owner the appropriate competitive "head start" to which he is entitled.[51] The application of the head start principle to the granting of injunctive relief results in a general conclusion that an injunction should not extend beyond the period of time that would be required to reverse engineer a product once it is on the open market.[52]

A particularly well-reasoned decision which explains the basis of the "head start" approach and indicates that the length of time required for reverse engineering is merely the starting place for determining the appropriate length of an injunction is *Analogic Corp. v. Data Translation, Inc.*[53] There, the court stated:

> Our holding today is not to be interpreted to require that the duration of an injunction be flexibly determined by the amount of time necessary to reverse engineer the plaintiff's device without improper use of trade secrets. But evidence as to this time period is one factor which should be considered in determining the reasonableness of the scope of such an injunction. Of course, defendants who have wilfully attempted to profit through violation of a confidential relationship need not be placed in as good position as other, honest competitors. '[T]he tendency of the law, both legislative and common, has been in the direction of enforcing increasingly higher standards of fairness or commercial morality in trade. The tendency still persists.' The plaintiff is entitled to have its trade secrets protected at least until others in the trade are likely, through legitimate business procedures, to have become aware of those secrets. And even then, the defendant should not be permit-

50. *See* Sperry Rand Corp. v. A-T-O, Inc., 447 F.2d 1387, 1392 (4th Cir. 1971) (duration of injunction held to be reasonable in light of evidence pertaining to the length of time required for independent development).

51. MILGRIM, *supra* note 1, at ¶ 2.01.

52. *See, e.g.*, Anaconda Co. v. Metric Tool & Dye Co., 485 F. Supp. 410, 429 (1980) (duration of injunction set at sixteen months to coincide with finding that this would be length of time for independent development); Data Gen. Corp. v. Digital Computer Controls, Inc., 297 A.2d 433 (Del. Ch. 1971), *aff'd*, 297 A.2d 437 (Del. 1972) (if injunction were granted, duration would be time required for reverse engineering); *see generally* MILGRIM, *supra* note 1, at ¶ 7.08[1] and cases cited in footnote 12.

53. 358 N.E.2d 804 (Mass. 1976) (reversing granting of permanent injunction).

> ted a competitive advantage from their avoidance of the normal costs of invention and duplication. Where the defendants have saved substantial expense by improperly using confidential information in creating their product, the ultimate cessation of an injunctive order might well be conditioned on their payment of an appropriate sum to the plaintiff. We mention this possibility to remind the lower courts of their creative equitable powers, and in no way intend to limit the scope of judicial discretion on remand.[54]

An important consideration is the question of who has the burden of establishing an appropriate length of time for an injunction. Clearly, the plaintiff must first establish that the product in question is sufficiently difficult to reverse engineer that it is entitled to trade secret protection. On the scope of injunctive relief, several courts appear to have held that it is the defendant's burden to show that it could, in fact, reverse engineer the product.[55]

One factor which may justify an injunction extending beyond the period required for reverse engineering, is the egregiousness of the defendant's activities.[56]

There is also case support for the proposition that the period for which damages are assessible also terminates after the expiration of the head start advantage gained by the misappropriator.[57]

### *d. Application of Reverse Engineering Principles to Mass Distributed Software*

Based on the principles of reverse engineering and trade secret accessibility set forth above, it is possible to construct an argument that mass-marketed software distributed without enforceable confidentiality agreements or in extremely large quantities should nonetheless be entitled to trade secret protection. This argument would be focused on the difficulty of obtaining the trade secrets embodied

---

54. *Id.* at 808 (citation omitted).

55. Carboline Co. v. Jarboe, 454 S.W.2d 540, 553 (Mo. Sup. Ct. 1970). *Accord*, Data Gen. Corp. v. Digital Computer Control, Inc., 357 A.2d 105, 114 (Del. Ch. 1975) (granting a permanent injunction where defendant was unable to carry its burden); Head Ski Co. v. KAM Ski Co., 158 F. Supp. 919, 924 (D. Md. 1958); Franke v. Wiltschek, 209 F.2d 493, 495 (2d Cir. 1953).

56. *See, e.g.*, Rego Displays, Inc. v. Fournier, 379 A.2d 1098, 1102-03 (R.I. 1977); Lincoln Steel Products, Inc. v. Shuster, 49 A.D.2d 618, 371 N.Y.S.2d 157 (1975); Analogic Corp. v. Data Translation, Inc., 358 N.E.2d 804 (Mass. 1976).

57. *See* Kubik, Inc. v. Hull, 56 Mich. App. 335, 224 N.W.2d 80 (1974); Structural Dynamics Research Corp. v. Engineering Mechanics Research Corp., 401 F. Supp. 1102 (E.D. Mich. 1975) (royalty damages imposed for period of time that would be required for independent development); Telex Corp. v. IBM Corp., 367 F. Supp. 258, 320-26, 359, 363 (N.D. Okla. 1973), *modified*, 510 F.2d 894 (10th Cir. 1974) (reversing antitrust aspects, affirming trade secret aspects, but modifying computation of damages).

in the object code of such software. The success of such an argument would depend on the following types of considerations:

(i) Was object code only distributed;

(ii) If object code only was distributed, how difficult would it be to "decompile" or "disassemble" such object code and how successful would such a process of "reverse engineering" be in laying bare the underlying trade secrets; and

(iii) What practical measures were taken to prevent copying and "decompilation" or "disassembly" of the object code.[58]

## III. APPLICATION OF TRADE SECRET PRINCIPLES IN EMPLOYER/EMPLOYEE CONTEXT

The courts have fashioned special rules regarding trade secrets in the employment context, which, for the most part, limit the employer's rights against the employee.[59]

### A. The Public Policy Protecting Employee Mobility

In order to prevail in an action for misappropriation of trade secrets, the plaintiff must not only show the existence of a trade secret, but also that the defendant gained access to that trade secret pursuant to, or in the course of, a covenant or confidential relationship imposing prohibitions on the defendant's subsequent use of that trade secret.[60] As will be more fully discussed, the principal basis on which such prohibitions arise in the context of employer/employee relationships is through a covenant of nondisclosure implied by law into the employment relationship or through the execution of an express covenant setting forth such prohibitions. Any such implied or express covenant will, however, be circumscribed in virtually all jurisdictions by judicially and legislatively adopted public policies solicitous of employee mobility. These policies have been described by one court as follows:

> The burden the appellees must thus meet brings to the fore a problem of accommodating policies in our law: The right of an individual to the unhampered pursuit of the occupations and livelihoods for which he is best suited. There are cogent socio-economic arguments in favor of either position. Society as a whole greatly benefits from technological improvements. Without some means of post-employment protection to assure that valuable developments or improvements are exclusively those of the employer, the businessman could not afford to subsidize research or improve current

58. *See supra* Section I.

59. *See also supra* Section I.C.

60. Wexler v. Greenberg, 399 Pa. 569, 160 A.2d 430 (1960); Futurecraft Corp. v. Clary Corp., 205 Cal. App. 2d 279, 23 Cal. Rptr. 198 (1962).

> methods. In addition, it must be recognized that modern economic growth and development had pushed the business venture beyond the size of the one-man firm, forcing the businessman to a much greater degree to entrust confidential business information relating to technological development to appropriate employees. While recognizing the utility in the dispersion of responsibilities in larger firms, the optimum amount of 'entrusting' will not occur unless the risk of loss to the businessman through a breach of trust can be held to a minimum.
>
> On the other hand, any form of post-employment restraint reduces the economic mobility of employees and limits their personal freedom to pursue a preferred course of livelihood. The employee's bargaining position is weakened because he is potentially shackled by the acquisition of alleged trade secrets; and thus paradoxically, he is restrained, because of his increased expertise, from advancing further in the industry in which he is most productive. Moreover, as previously mentioned, society suffers because competition is diminished by slackening the dissemination of ideas, processes and methods.[61]

In California, the courts have created a special rule which must be applied when one of the defendants to a trade secret action is a former employee of plaintiff:

> One who seeks protection against the use or disclosure of a trade secret must plead facts showing (1) the existence of subject matter which is capable of protection as a trade secret; (2) the secret was disclosed to the defendant, under circumstances giving rise to a contractual or other legally imposed obligation on the part of the disclosuee not to use or disclose the secret to the detriment of the discloser, and *(3) if the defendant is an employee or former employee of the plaintiff . . . the facts alleged must show that the public policy in favor of the protection of the complainant's interest in maintaining the secret outweighs the interest of the employee in using his knowledge to support himself in other employment . . . .*[62]

---

61. Wexler v. Greenberg, 399 Pa. 569, 160 A.2d 430, 434 (1960).

62. Diodes, Inc. v. Franzen, 260 Cal. App. 2d 244, 250, 67 Cal. Rptr. 19, 25 (1968) (emphasis added). *See also* Kalinowski, *Key Employees and Trade Secrets*, 47 VA. L. REV. 583, 599 (1961) ("Protection should be afforded when, and only when, the information in question has value in the sense that it affords the plaintiff a competitive advantage over competitors who do not know of it, and where the granting of such protection will not unduly hamstring the ex-employee in the practice of his occupation or profession. This simple balancing process will invariably protect all of the pertinent interests—those of the former employer, of the former employee, and of the public."); Wear, *A Balanced Approach to Employer-Employee Trade Secret Disputes in California*, 31 HASTINGS L.J. 671 (1980); MILGRIM, *supra* note 1, at ¶ 5.02.

### B. Determining the Scope of an Employee's Duty Not to Disclose or Use Trade Secrets of a Former Employer

The courts have also fashioned special substantive and procedural rules which refine the scope of an employee's duty of non-disclosure with respect to a former employer's trade secrets.

#### *1. Implied Covenant of Non-Disclosure in Employer/Employee Relationship*

An employer seeking to establish trade secret misappropriation by a former employee in developing a competing product either for his own use or for use by a subsequent employer must show that development of the product was accomplished through the improper use of trade secret information rather than through independent development utilizing general information. The mere disclosure of trade secret information by the owner of such information to a third party does not, however, impose a restriction on such third party not to use or disclose such information. As discussed above, the general rule is that the trade secret status of information is lost if it is disclosed without some form of restriction on use or disclosure.

Despite the general rule that trade secret status is lost if the secret is disclosed, no such loss occurs where the disclosure follows from or is made in the context of an employer/employee relationship since there is, in every employment relationship, an implied covenant preventing employees from utilizing for their benefit or the benefit of others any trade secrets to which they received access in the course of their employment.[63] The existence of such a covenant prevents an employer from losing trade secret protection for information disclosed to an employee in the course of his employment and provides a legal basis on which to bring an action for trade secret misappropriation in the event that an employee uses such information for his own or a subsequent employer's benefit.

##### *a. Limitations on Implied Covenant of Non-Disclosure*

Both in view of the public policy against limitations restricting employee mobility and the inherently ambigous nature of implied covenants, the courts have developed various rules limiting the scope of such a covenant. These limitations are significant not only in cases where an employer seeks to base a claim on the implied

63. *See* By-Buk Co. v. Printed Cellophane Tape Co., 163 Cal. App. 2d 157, 329 P.2d 147 (1958) (former employee of plaintiff and his new employer held liable for misappropriation of plaintiff's trade secret despite absence of express non-disclosure covenant, since such a covenant is implied by law). *See generally*, Milgrim, *supra* note 1, at ¶ 5.02[1].

covenant of non-disclosure, but also as a background for understanding the additional protection which may be available to an employer through use of written covenants.

*(1) Difficulty of Establishing the Existence of Trade Secret*

The most significant limitation on the implied covenant of non-disclosure in employment relationships is the problem, discussed in detail below, of showing that alleged trade secret information is in fact a trade secret as opposed to general information relating to the type of job the employee performs. As will be discussed below, express covenants of non-disclosure and covenants not to compete can to a certain degree moot this issue.

*(2) Notice of Confidential Nature of Information*

While the implied covenant of non-disclosure in the employment relationship will operate to prevent use by a former employee of trade secret information, it does not specifically describe what information the employer considers to be trade secret in nature. It is unlikely that an employee ignorant of the trade secret nature of the information to which he receives access in the course of his employment will be found liable for wrongful post-employment use of such information. In the absence of an express covenant specifying the trade secret nature of specific information, an employer will, in establishing a case for trade secret misappropriation based upon an implied covenant of non-disclosure, have to establish notice by relying upon (i) the context in which such information is disclosed to the employee, (ii) the measures taken by the employer to protect the secret status of the information, or (iii) knowledge which the employee can, based upon industry standards, reasonably be expected to possess as to what provides one employer with a competitive advantage over his competitors.[64]

Given the generally high level of concern exhibited by most employers over their software (e.g., restrictive licensing agreements; non-dissemination of source code; confidentiality legends on human-readable versions of the software; and in-house security measures), it should not be too difficult for employers, in most circumstances and even in the absence of express covenants, to establish the fact that an employee receiving access to or developing software in the

64. *See* MILGRIM, *supra* note 1, at ¶ 5.02[2], *citing* Shatterproof Glass Corp. v. Guardian Glass Co., 322 F. Supp. 854 (E.D. Mich. 1970), *aff'd*, 462 F.2d 1115 (6th Cir. 1972).

course of his employment should have understood and been on notice of the confidential nature of such software.

It is, however, interesting to speculate on the outcome of this issue in circumstances such as the following:

(i) Despite contractual prohibitions against unauthorized use or disclosure of its software, an employer has a history of not enforcing its rights against former employees or other third parties who violate such prohibitions.

(ii) Software is written in such a basic language that the distinction between source and object code is meaningless and anybody receiving access to the software in machine-readable form would effectively possess in human understandable terms the basic logic and coherence of the software. In such a situation, an employee could plausibly argue that the employer could not, in light of his marketing strategy, realistically expect to maintain the confidential nature of the software.

(iii) The employer stops actively marketing or promoting a certain software package.

#### *(3) High-Level Versus Low-Level Employees*

Although the confidential relationship giving rise to the duty of non-disclosure implied in the employment relationship clearly applies to high level employees where the need for trust and a fiduciary relationship between employer and employee is critical to the performance of the employee's duty, at least one case suggests that a low paid hourly employee might not enjoy a confidential relationship with his employer.[65] It would not be surprising to find a part time programmer working on an hourly basis for a particular employer defending a trade secret action brought by the employer on the grounds that, in the absence of an express covenant, the context of his employment did not involve a confidential relationship sufficient to support an implied covenant of non-disclosure. Given the general sensitivity of the software industry to confidentiality and assuming that the employer utilizes some protective measures indicating the confidential nature of the software, this argument should rarely be persuasive in software related cases.

### C. The Employee as Developer Rather Than Disclosee of Trade Secret Information

The difficult issues with respect to trade secret rights in an employer/employee relationship are further complicated when the em-

65. Bull v. Log Elec., Inc. 323 F. Supp. 115 (E.D. Va. 1971), *cited in* Milgrim, *supra* note 1, at ¶ 5.02[1], n.10.2.

ployee is also the developer of the trade secrets, as opposed to simply a disclosee of such trade secrets.

### *1. General Rules as to Ownership of Employee-Developed Trade Secrets*

A significant body of law has developed regarding the respective rights of an employer and employee to patentable inventions developed by the employee, in the absence of an express written agreement to the contrary.

(i) The general rule is that the proprietary rights to inventions produced by an employee pursuant to employment in which he is told to make such an invention belong to the employer.[66]

(ii) Absent a contractual provision to the contrary, it is the general rule that the proprietary rights to inventions made by an employee who is simply hired to make inventions without any more specific direction also belong to the employer.[67]

(iii) At least in superficial contradiction to the foregoing principles, it is also generally accepted that proprietary rights to inventions made by employees using their employer's materials, facilities or personnel during the course of employment remain the employee's property unless by the terms of his employment or otherwise the employee agreed that such rights belong to his employer.[68] This principle is reconciled with those set forth above in that, in the absence of express agreement, courts will look to the nature and scope of the employment relationship to determine whether there is an implied agreement by the employees to assign over the proprietary rights by the employees to assign over the rights in their inventions. Such an implied agreement is readily found in the circumstances described in (i) and (ii) above.[69]

(iv) Where an employee develops an invention outside the course of his employment or without any implied or express agreement to assign, but uses the employer's facilities, personnel or materials to create the invention, the "shop rights" doctrine may provide the employer with a non-exclusive right to use the invention.[70]

Although there is little case law on the subject, it would appear that the reasoning underlying the above principles with respect to patentable inventions should be applicable to trade secrets.

---

66. *See* MILGRIM, *supra* note 1, at ¶ 5.02[4].
67. *Id.*
68. *Id.*
69. *Id.*
70. *Id.*

*2. Special Problem of Software Developer/Employee*

In the absence of an express written agreement to assign, trade secret litigation against an employee who develops software in the course of his employment has produced judicial decisions which appear inconsistent with the principles set forth in the immediately preceding section.

Unlike hardware, which is often designed by a large number of employees, software is often developed by a few, or perhaps only one person. Courts have sometimes held that the programmer has as much right to the trade secrets inherent in a program as does his employer.

In *Structural Dynamics Research Corp. v. Engineering Mechanics Research Corp.*,[71] plaintiff corporation sued three former employees for, *inter alia*, misappropriation of trade secrets in a program for solving structural analysis problems. One of the employees had suggested that the corporation develop such a program at a time when no other employee in the corporation had any significant knowledge of the mathematical theories necessary to such development. That employee and the other two employees named as defendants in the action subsequently developed the program without other assistance from plaintiff.

The trial court cited societal concerns in preserving the job mobility of technically skilled employees who might be "less attractive to new employers so far as their acquired skills and knowledge are regarded as trade secrets,"[72] and then held that the employees here did not obtain trade secrets through "improper" means, since in substantial measure they were the "developers and innovators" of the trade secret program:

> [I]f the subject matter of the trade secret is brought into being because of the initiative of the employee in its creation, innovation or development even though the relationship is one of confidence, no duty arises since the employee may then have an interest in the subject matter at least equal to that of his employer or in any event, such knowledge is a part of the employee's skill and experience. In such a case, absent an express contractual obligation by the employee not to use or disclose such confidential information acquired during his employment adverse to his employer's interest, he is free to use or disclose it in subsequent employment activity . . . . Where the employer assigns the employee to a specific development task and commits considerable resources and supervision to the project, a confidential relationship arises that prevents the employee from using or disclosing the fruits of his research. When, on

71. 401 F. Supp. 1102 (E.D. Mich. 1975).
72. *Id.* at 1111.

> the other hand, the developments are the product of the application of the employee's own skill, "without any appreciable assistance by way of information or great expense or supervision by [the employer], outside of the normal expenses of his job," he has "an unqualified privilege" to use and disclose the trade secrets so developed.[73]

The court did, however, find that the employees were nonetheless liable for breach of specific contractual provisions preventing them from disclosing the trade secrets, thereby underscoring the potential advantages (more fully discussed below) of suing for the breach of an express non-disclosure covenant rather than relying on a breach of the covenant of non-disclosure implied in the employer/employee relationship.

The decision in *Structural Dynamics* seems inconsistent with the rules applied in patent cases insofar as the defendant employees were clearly developing the software in the course of their employment with plaintiff while drawing a salary for work on that specific development project. Despite these facts, the court supported the proposition that, absent an express contractual provision to the contrary, the developer employees could not be enjoined from using the fruits of their effort. The conceptual underpinning for the distinction made by the court in *Structural Dynamics* between the scope of implied covenants with respect to an employee who develops rather than simply receives access to his employer's trade secrets was comprehensively articulated by the Supreme Court of Pennsylvania in *Wexler v. Greenberg*,[74] quoted with approval in a leading California trade secret case as follows:

> We are initially concerned with the fact that the final formulations claimed to be trade secrets were not disclosed to Greenberg by the appellees during his service or because of his position. Rather, the fact is that these formulas had been developed by Greenberg himself, while in the pursuit of his duties as Buckingham's (i.e., plaintiff's) chief chemist, or under Greenberg's direct supervision. We are thus faced with the problem of determining the extent to which a former employer, without the aid of any express covenant, can restrict his ex-employee, a highly skilled chemist, in the uses to which this employee can put his knowledge of formulas and methods he himself developed during the course of his former employment because this employer claims these same formulas, as against the rest of the world, as his trade secrets. This problem becomes particularly significant when one recognizes that Greenberg's situation is not uncommon. In this era of electronic, chemical, missile and atomic development, many skilled techni-

73. *Id.* at 1111-12 (citations omitted).

74. 399 Pa. 569, 160 A.2d 430 (1960).

> cians and expert employees are currently in the process of developing potential trade secrets. Competition for personnel of this caliber is exceptionally keen, and the interchange of employment is commonplace. One has but to reach for his daily newspaper to appreciate the current market for such skilled employees. We must therefore be particularly mindful of any effect our decision in this case might have in disrupting this pattern of employee mobility, both in view of possible restraints upon an individual in the pursuit of his livelihood and the harm to the public in general in forestalling to any extent widespread technological advances. . . .
>
> The sole issue for us to decide, therefore, is whether or not a confidential relationship existed between Greenberg and Buckingham binding Greenberg to a duty of nondisclosure.
>
> The usual situation involving misappropriation of trade secrets in violation of a confidential relationship is one in which an employer discloses to his employee a pre-existing trade secret (one already developed or formulated) so that the employee may duly perform his work. In such a case the trust and confidence upon which legal relief is predicated stems from the instance of the employer's turning over to the employee the pre-existing trade secret. It is then that a pledge of secrecy is impliedly extracted from the employee, a pledge which he carries with him even beyond the ties of his employment relationship. Since it is conceptually impossible, however, to elicit an implied pledge of secrecy from the sole act of an employee turning over to his employer a trade secret which he, the employee, has developed, as occurred in the present case, the appellees must show a different manner in which the present circumstances support the permanent cloak of confidence cast upon Greenberg by the Chancellor.[75]

In *Wexler*, the court concluded that the defendant employee Greenberg was entitled to disclose and use the formulas which he had developed in the course of his employment since they were a part of the technical knowledge and skill which he had acquired by virtue of his employment—even though the formulas were acknowledged by the court to constitute trade secrets of plaintiff.

While the decision in *Wexler* has been criticized in view of the specific facts before the court,[76] there may in fact be merit to the court's recognition that the employee/developer of a trade secret has a more compelling basis on which to continue use of a trade secret after termination of his employment than does a disc-

75. Futurecraft Corp. v. Clary Corp., 205 Cal. App. 2d 279, 284-86, 23 Cal. Rptr. 198, 208-09 (1962) (citations omitted).

For cases prohibiting disclosure or use by employees of alleged trade secret information developed at least in part through their efforts, *see* Extrin Foods, Inc. v. Leighton, 202 Misc. 592, 115 N.Y.S.2d 429 (1952); Wireless Specialty Apparatus Co. v. Mica Condenser Co., Ltd., 239 Mass. 158, 131 N.E. 307 (Mass. 1921).

76. *See* Note, 74 HARV. L. REV. 1473 (1961); MILGRIM, *supra* note 1, at ¶ 5.02[3].

losee/employee. The distinction between the general knowledge or skills of a particular profession and specific information relating to a single employer is often very difficult to draw. It is certainly arguable that, as the court in *Wexler* indicates, such a distinction is even more difficult to make when it is the expertise of the developer which produces the trade secret. Moreover, since the developer/employee's livelihood consists of utilizing such expertise on a continuing basis, the policy against restrictions preventing employee mobility should be to require a particularly rigorous scrutiny of information alleged to be trade secrets to determine whether or not the classification of such information as a trade secret unduly hampers the developer/employee's mobility.

By way of example, a programmer skilled in developing medical claims processing software who is hired by an employer to develop such a software system will be particularly vulnerable to such employer later claiming trade secrets in the program developed for him since it is inevitable that such employee will not be able to find subsequent employment in the medical claims software area not requiring him to utilize certain skills which reside in the gray area of specific versus general knowledge. The plight of such a programmer should be contrasted with that of a salesman hired by the same employer to market the system. Clearly, such a salesman can be held to a stricter standard of non-disclosure since his subsequent employment will not require him to utilize the specifics of his former employer's system, but only to market what his subsequent employer had developed independent of him.

### D. Express Covenants of Non-Disclosure and Non-Competition

The principal limitations circumscribing the scope of implied covenants of trade secret non-disclosure in the employer/employee relationship have been described above as (i) the difficulty of establishing the existence of a trade secret rather than general information, (ii) notice to the employee of what information cannot be disclosed, (iii) the possible lack of a confidential relationship giving rise to an implied covenant of non-disclosure between the employer and low-level employees, and (iv) the possibility of developer/employees claiming proprietary rights in the items they develop. Through use of express covenants executed by the employee, each of these limitations can be materially limited in potential impact.

### *1. Covenants Not to Compete Offering Broader Protection than Covenants Not to Disclose*

In most jurisdictions, employee covenants not to compete have been upheld when they are not broader than necessary to protect the employer's legitimate business interests. Generally, covenants not to compete have been enforceable in a trade secret context when the intent of the covenant is to prevent the employee from working in areas (i) where it would be difficult to determine if he was using specific trade secret information of his former employer or general information related to his profession, or (ii) where it would be difficult for him to avoid using his former employer's trade secret information in the course of his employment and enforcement of a simple covenant not to disclose would therefore not be sufficient to protect the employer's interest.

Thus, in *Modern Controls, Inc. v. Andreadakis*,[77] plaintiff Modern Controls brought an action against its former employee, Andreadakis, to enforce a covenant not to compete which would prevent Andreadakis from working for Modern Control's competitor, Burroughs Corporation. In overturning the district court's finding that the covenant not to compete was unenforceable because the device which Andreadakis worked on for Modern Controls (a flat panel gas discharge display device used to display information from a computer to a computer user) did not contain any trade secret, the court of appeals held as follows:

> The Minnesota Supreme Court has held that confidential business information which does not rise to the level of a trade secret can be protected by a properly drawn convenant not to compete. (citations) To require an employer to prove the existence of trade secrets prior to enforcement of a covenant not to compete may defeat the only purpose for which the covenant exists. An employer need only show that an employee had access to confidential information and a court will then determine the overall reasonableness of the covenant in light of the interest sought to be protected. Eutectic Welding Alloys Corp. v. West, 281 Minn. 13, 18-20, 160 N.W.2d 566, 570-571 (1968). Modern Controls has established by affidavit that Andreadakis had access to confidential business information.
>
> Andreadakis claims that he and the persons he was working with developed no confidential business information during his employment that he did not already know. He argues that he left Modern Controls with no more information than he possessed when he left Control Data. The affidavits submitted by Andreadakis do not support this contention. To the contrary, the unrefuted evidence shows that during the time of his employment, the device moved

77. 578 F.2d 1264 (8th Cir. 1978).

> from an unmarketable state to a marketable one and that this transition was accomplished after Modern Controls invested over $500,000 and utilized approximately one-half, or seventeen, of its employees over a sixteen-month period.[78]

The court's opinion in this case is significant insofar as it suggests that a covenant not to compete can be utilized to prevent the disclosure of confidential as opposed to trade secret information. The critical conceptual distinction underlying the court's opinion is that the covenant not to compete was not viewed by the court as simply preventing competition by Andreadakis through use of confidential information, but as preventing competition generally as a result of Andreadakis's access to such confidential information. In this context, the court was not concerned over whether or not such information was generally known in the industry or would have been acquired by Andreadakis in the course of similar employment with an alternative employer. In view of the inevitable difficulty of distinguishing generic from specific information in software related trade secret actions, the potential ability to obtain broad protection for business information through use of a covenant not to compete, without the often insurmountable burden of providing trade secret status for such information, represents a significant benefit to be derived through use of a written covenant not to compete to supplement covenants against non-disclosure. It is interesting to note in this context that authority also exists for the proposition that a written covenant not to disclose may provide employers with similarly expanded coverage with respect to information that may not rise to the level of a trade secret, but only to the extent of preventing disclosure of such confidential information rather than competition in which such disclosure might be difficult to avoid or detect.[79]

Since covenants not to compete which are broader than necessary to protect an employer's legitimate interests will not be enforced in view of the public policy against restrictions on employee mobility, the court in *Modern Controls* had to face the issue of whether or not Modern Controls had established that enforcement of the covenant not to compete was necessary to prevent disclosure by Andreadakis of Modern Control's confidential or trade secret information:

> The District Court also denied relief on the ground that Modern Controls had failed to show irreparable harm because it had not established that Andreadakis had disclosed or would disclose trade

78. *Id.* at 1268-69 (citations and footnotes omitted).

79. *See* Maloney v. E.I. du Pont de Nemours & Co., 352 F.2d 936, 938 n.4 (D.C. Cir. 1965, *cert. denied*, 383 U.S. 948 (1966)); MILGRIM, *supra* note 1, at ¶ 3.02[1] n.12 and accompanying text.

> secrets or confidential business information gained at Modern Controls to Burroughs. Andreadakis emphasizes on appeal that Burroughs specifically instructed him not to disclose any trade secrets and that since he has already worked for Burroughs for about a year without disclosing any trade secrets or other confidential information, it is unlikely that he would do so in the future.
>
> The possible disclosure of trade secrets and confidential information is certainly relevant in determining the potential harm to any employer. However, such information may be disclosed in more subtle ways than outright disclosure to a third party. As Professor Harlan M. Blake noted,
>
> > [e]ven in the best of good faith, a former technical or "creative" employee working for a competitor, or in business for himself in the same or a related field, can hardly prevent his knowledge of his former employer's confidential methods or data from showing up in his work. And utmost good faith cannot always be expected. (citation).
>
> It is unrealistic to expect that Andreadakis has not utilized confidential information gained at Modern Controls when working on an identical product at Burroughs. It is equally unrealistic to expect that this confidential information will not give Burroughs a significant advantage over its significantly smaller competitor. Burroughs has the capacity to devote a large amount of its resources to the development of a competing device that would eliminate Modern Controls' competitive advantage. Andreadakis's knowledge would be invaluable in this respect. These factors lead to the conclusion that Modern Controls will suffer irreparable harm.[80]

The basic point made by the court in *Modern Controls* is that an employee with access to one employer's confidential and trade secret information cannot realistically be expected not to utilize or disclose such information when working for a subsequent employer in the same capacity. Accordingly, a mere covenant not to disclose (whether implied or express) cannot, in such circumstances, be said to protect all of the former employer's legitimate business interests. In the same way as the expanded subject matter coverage offered by a covenant not to compete is particularly appropriate in a software context where the distinction between general and specific knowledge is often very murky, the use of covenants not to compete to avoid the question of "inevitable disclosure" and related evidentiary

80. 578 F.2d at 1269-70 (citations omitted). *See* Blake, *Employee Agreements Not to Compete*, 73 HARV. L. REV. 625, 669-70 (1960). *See also* A. Hollander & Son, Inc. v. Imperial Fur Blending Corp., 2 N.J. 235, 66 A.2d 319 (1949), *cited in* MILGRIM, *supra* note 1, at ¶ 3.02[1] n.24 ("the validity of the covenant is not predicated on methods secret in fact and revealed to the employee in confidence but rests on the protection afforded an employer against disclosure of business and industrial methods and processes used, records compiled and customer contacts made in the employment").

issues is also particularly justified. This precise point is made in a software context by the court in *Electronic Data Systems Corp. v. Powell*,[81] through emphasis on both the practical inability of the employee to avoid or the former employer to detect disclosure and the conflicting promises of loyalty the employee made to his former and current employers:

> Appellant's [EDS's] business of employing systems engineers to write computer programs for its customers is unique and highly specialized. Its training of Powell included specialized information pertaining to its business as distinguished from general skills and knowledge of the trade. Restraining him from using this information is intrinsically unenforceable so long as he is employed by a competing employer in the health-care field. It would indeed be difficult to determine if Powell were imparting his specialized knowledge to SRI [the subsequent employer] until SRI markets a product resembling closely EDS's system.
>
> The evidence on the merits reveals that Powell, by participating in the servicing of SRI medicare contracts, preparing SRI proposals to process health care claims for potential EDS customers, including a proposal to incorporate utilization review into the system operated by SRI for Kansas City Blue Shield, and participating in the development and marketing of an SRI computer system for processing regular business healthcare claims, has violated his covenant not to compete with EDS. All of these activities were admitted by Powell.
>
> It was clearly established that the methods and techniques developed by EDS have resulted from a significant investment of time and money. Even in the best of good faith, a former technical or "creative" employee such as Powell working for a competitor such as SRI can hardly prevent his knowledge or his former employer's confidential methods from showing up in his work [citation omitted]. If Powell is permitted to work for SRI in the same area as that in which he was trained by EDS, injunctive relief limited to restraint of imparting such special knowledge as prepayment utilization review, is likely to prove insufficient. The mere rendition of service in the same area would almost necessarily impart such knowledge to some degree in his subsequent employment. Powell cannot be loyal both to his promise to his former employer, EDS, and to his new obligation to his present employer, SRI. In these circumstances, the most effective protective device is to restrain Powell from working in the same computer field in which he was associated while employed by EDS.[82]

---

81. 524 S.W.2d 393 (Tex. Civ. App. 1975).

82. *Id.* at 398. *See also*, Harrison v. Glucose Sugar Ref. Co., 116 F. 304 (7th Cir. 1902) (superintendent for manufacturer of glucose, starch, grape, sugar and similar products enjoined from violating post-employment covenant not to compete in view of inevitable breach of covenant not to disclose secret information); Ideal Laundry

*2. Limitations on the Use of Covenants Not to Compete*

It is important to recognize that use of a covenant not to compete to supplement an express or implied covenant of non-disclosure is not by any means the solution to all of the difficulties besetting a trade secret plaintiff in an action against his former employees. Several limitations on the use of covenants not to compete must be considered in evaluating the effectiveness of such a covenant.

*a. Adequacy of Consideration*

As the following portion of the opinion in *Modern Controls, Inc. v. Andreadakis*[83] indicates, there is some question as to whether covenants not to compete (and perhaps the expanded protection offered by an express covenant not to disclose) entered into after the commencement of employment are supported by adequate consideration:

> Whether a covenant not to compete entered into after employment has commenced is supported by independent consideration is a question that has evoked considerable disagreement in the courts. Many courts support the position that continued employment constitutes sufficient consideration for a covenant not to compete. Annot., 51 A.L.R.3d 825, 835-839 (1973); Blake, *Employee Agreements Not to Compete*, 73 Harv. L. Rev. 625, 669 n.145 (1960). Other courts require something in addition to the mere continuance of employment. Annot., 51 A.L.R.3d 825, 833-835 (1973). This "something in addition" may be a raise, a new position or an increased employment term. The Minnesota Supreme Court has not yet determined whether continued employment alone is sufficient consideration for a covenant not to compete. We need not predict what the Minnesota Court would do, however, as the covenant not to compete was supported by something more than the mere continuance of employment. It was supported by an obligation on the part of Modern Controls to pay Andreadakis his base pay for two years if he could not find suitable work in another field.[84]

*b. Overbreadth*

In recognition of the fact that covenants not to compete are at

---

Co. v. Gugliemme, 107 N.J. Eq. 108, 151 A. 617 (1930) (plaintiff's former employee enjoined from continuing work with plaintiff's competitor where subsequent employer hired employee specifically to obtain plaintiff's confidential information); National Starch Products v. Polymer Indus., 273 A.D. 732, 79 N.Y.S.2d 357 (1948), *rearg'd and appeal denied*, 274 A.D. 822, 81 N.Y.S.2d 278 (1948); Annot., 30 A.L.R.3d 631.

83. 578 F.2d at 1267-68.

84. *See* discussion *supra* in Section I.C for additional citations and practical suggestions for dealing with this problem.

odds with the public policy against post-employment restrictions, courts will generally refuse to enforce such covenants if they go beyond what is required to protect the employer's reasonable business needs as to subject matter, geographic effect or duration. It should also be noted that the problem of overly broad post-employment restrictions is not confined to covenants not to compete but can arise with respect to overly broad covenants not to disclose. While certain courts may flatly refuse to enforce overly broad post-employment covenants, the better rule is that courts will judicially construe the covenant to extend only as far as it is necessary to protect the employer's reasonable business interests.[85]

*c. Void as Against Public Policy*

In certain jurisdictions such as California, any post-employment covenant not to compete (with certain exceptions generally related to the sale of the goodwill of a business) is void as against public policy.[86] In such jurisdictions, a former employer must rely on the more limited protection afforded by covenants not to disclose as the principle means of protecting against misappropriation of trade secrets by former employees.

*d. Narrow Substantive Scope of Injunction*

While courts are frequently willing to enforce covenants not to compete through the issuance of injunctions in situations where inevitable disclosure of trade secrets would occur, the substantive scope of such injunctions is typically limited to the narrowest possible restraint necessary to protect the former employer's legitimate business interest.[87] In fact, a court is more likely to enforce a covenant not to compete if it can be structured to permit the employee to continue working in a general field only a portion of which is foreclosed by virtue of the covenant.[88] This principle applies with equal force to injunctions issued to enforce a simple covenant not to dis-

85. *See generally* MILGRIM, *supra* note 1, at ¶ 2.02[2].

86. *See* Cal. Bus. & Prof. Code § 16600 (West 1964).

87. *See* Electronic Data Sys. v. Powell, 524 S.W.2d 393 (Tex. Civ. App. 1975) (employee restricted from working only in that portion of data processing industry related to health care industry).

88. *See* Allis Chalmers Mfg. Co. v. Continental Aviation & Eng'g Corp., 255 F. Supp. 645 (E.D. Mich. 1966) (applying Michigan law) (action by manufacturer of distributor-type pump for fuel injection systems against former employee for misappropriation of trade secrets related to production of such pumps; injunction issued permitting employee to work for competitors in all fields of application engineering and to participate in the development of all types of fuel injection systems except distributor-type pump). *But see* Heyden Chem. Corp. v. Burrell & Neidig, 2 N.J. Super. 467, 64 A.2d 465 (1949).

close as opposed to the more restrictive covenant not to compete.[89]

From the foregoing analysis, it can be assumed that a court faced with fashioning injunctive relief intended to protect an employer's trade secrets in a particular piece of software will seek to limit the scope of such injunctions to the development of functionally similar software. Thus, a programmer who developed a medical billing system for his former employer may be enjoined from developing another medical billing system, but not from developing a legal billing system. While such an approach may in many circumstances be adequate to protect the former employer's interest, it is possible that the distinction between, for example, a medical billing system and a legal billing system may ignore the fact that much of the "unique logic and coherence" in a medical billing system (e.g., the portion consisting of a sophisticated data base management system) may be extremely valuable in the design of a legal billing system. While an injunction merely preventing disclosure of trade secrets would, by its terms, apply to such disclosure for purposes of developing the legal system, enforcement of a covenant not to compete should probably not extend to development of a legal billing system unless the former employer was in fact engaged in or likely to engage in marketing or developing such a system. In the absence of such facts, it is difficult to see how the employee could be viewed as "in competition" with his former employer simply by engaging in the development of a legal billing system.

### *3. Use of an Express Non-Disclosure Covenant to Establish Confidential Relationship with Low-Level Employees*

As discussed above, courts may be reluctant to find a confidential relationship between an employer and low-level employees sufficient to support an implied covenant of non-disclosure. In such circumstances, as well as in other instances where it is unclear as to whether or not information is disclosed pursuant to a confidential relationship (e.g., disclosure to an independent contractor), execution of an express agreement acknowledging the existence of such a relationship and the confidential nature of the information disclosed pursuant thereto can significantly assist an employer in establishing a legal basis on which to ground a claim for misappropriation of

89. *See* By-Buk Co. v. Printed Cellophane Tape Co., 163 Cal. App. 2d 157, 329 P.2d 147 (1958) (injunction restraining employee from acquiring or using any machine similar to machines manufactured by his former employer held too broad). A good summary of the wide disparity in the scope of injunctive relief granted in trade related cases is provided in Annot., 30 A.L.R.3d 631. *See also* Berryhill, *Trade Secret Litigation: Injunctions and Other Equitable Remedies*, 48 U. COLO. L. REV. 189 (1977).

trade secrets.[90]

### 4. *Use of Written Agreement to Establish Ownership of Employee Developed Information or Knowledge*

An express agreement pursuant to which an employee assigns all right, title and interest in and to any and all inventions, discoveries and developments made in the course of his employment can substantially reduce the risk of a court determination that a developer/employee is entitled to continuing use of developments which he makes in the course of his employment.[91]

### 5. *Use of Written Agreement to Put Employee on Notice of Trade Secret Ownership*

In his widely cited treatise on trade secrets, Roger Milgrim succinctly summarizes methods of use of written agreements to give notice to employees of trade secret claims, thereby reducing at least one of the problems discussed above with respect to non-disclosure covenants as follows:

> A written agreement clearly and unequivocally puts an employee or an independent contractor on notice of the trade secret owner's claims. Many large corporations, through their personnel departments, explain to new employees the reasons for a patent assignment and secrecy agreement. The theory for doing this is apparently threefold. (1) It is felt that a fair explanation will assure the most favorable employer/employee relations. (2) It makes the employee 'secrecy' conscious, and hopefully will induce him to exercise prudence with reference to confidential matters. (3) It establishes a standard business procedure which, in the event of litigation respecting alleged violation of trade secret information, might have evidentiary value tending to prove that the employee was on notice. In a sense, standard use of a written employment agreement will create a rebuttable presumption that an employee was on notice of its terms even where the employee may claim to have forgotten signing the agreement. Care should be taken, however, to regularly acquaint an employee with the fact that he is being asked to sign a restrictive covenant and its meaning.[92]

---

90. *See generally* MILGRIM, *supra* note 1, at ¶ 3.20[1][6].

91. *See* Structural Dynamics Research Corp. v. Engineering Mechanics Research Corp., 401 F. Supp. 1102 (E.D. Mich. 1975) (developer employees who would otherwise be entitled to continue use of software programs and related information they developed, held liable for breach of express covenant prohibiting such use).

92. MILGRIM, *supra* note 1, at ¶ 3.02[1][C].

## IV. ENFORCING TRADE SECRET RIGHTS—THE PRACTICAL PROBLEMS

Distinguishing between generic knowledge, which is not protectible as a trade secret, and specific knowledge comprising the unique logic and coherence of software is very difficult. In large part this difficulty is a result of the fact that a substantial portion of all software developed for commercial use is functionally similar to other software on the market and simply reflects the dedicated application of generally known programming skills over a considerable period of time. The difficulties presented by such functional similarity are compounded by the fact that a programmer intending to conceal his acts of misappropriation can easily disguise such acts by various means:

> Most courts do not possess sufficient technical background to determine whether striking similarities exist between seemingly dissimilar works. Therefore, expert witnesses are generally permitted to testify concerning the degree of similarity, or lack thereof, between the programs. Even experts, however, find it extremely difficult to determine if one computer program has been copied from another. If the plaintiff could find one expert who was willing to testify to striking similarities, the defendant could, no doubt, get two to swear to the contrary. The same computer process can appear in a bewildering array of forms including the flow chart, source program and object program. Both the source and the object programs can appear on a variety of media including magnetic tape, cards, and disk. The source program can be written in an ever increasing number of high level languages, e.g., FORTRAN, BASIC, ALGOL, COBOL, etc. There are even 'dialects' of the source languages which vary with the computer operation. Even two source programs written in the same language and which do precisely the same job can be markedly different. They can differ in all the following respects: the order and manner in which data is to be entered, the variable names, the order of instructions, the statement numbers, the way in which the same instruction can validly be expressed, the number and formulation of comment statements, and the format of the output. They could have different underlying algorithms (in which case copying is highly unlikely), and each could require the use of different input or output devices. All of these differences must be explained to, considered, and weighed by a trier of fact who has at best a minimal understanding of the source language and the technical terminology.[93]

93. Gemignani, *Legal Protection for Computer Software: The View from '79*, 7 RUT. J. COMPUTER TECH. & L. 269, 288-89.

### A. Narrowing the Focus to Only the Trade Secret Elements of Software

As discussed above, the attention of a trade secret plaintiff should not be addressed broadly to the misappropriation of software, but rather should be focused on the misappropriation of the trade secret elements of such software. Such elements include: (i) the unique logic and coherence of the software producing a certain level of "commercial feasibility," (ii) the competitive "head start" represented by a plaintiff's investment of time and effort in order to develop or acquire the use of the software, and (iii) the development and programming of novel algorithms allowing the application of data processing technology to new functions.

### B. Discovery of the "Smoking Gun"

In *University Computing Co. v. Lykes-Youngstown Corp.*,[94] the factual findings upon which the court ultimately found trade secret misappropriation by the defendants were in substantial part described as follows:

> Following the incorporation of LYCSC (the newly created subsidiary of LYC) the new corporation proceeded to offer AIMES III to customers. Rather than purchase unrestricted rights to the system for UCC, LYCSC elected to steal the system from Leonard's. In December, 1969, LYCSC bribed an employee of Leonard's for $2500 to deliver a suitcase filled with computer tapes and other materials to an employee of LYCSC. In February, 1970, this same Leonard's employee was paid to fly to Atlanta from Dallas with additional tapes and documents once the materials originally obtained were found to be insufficient to run the system. With the new materials and the help of the Leonard's employee in installing the system in the LYCSC in-house computer, LYCSC was able to run the system in its entirety.[95]

In *Telex Corp. v. IBM Corp.*,[96] one of the principal factual findings resulting in judgment against Telex for misappropriation of IBM's trade secrets in certain software was summarized by the court as follows:

> The trial court also found that Telex had misappropriated the source code to IBM's "FRIEND" version 2 diagnostic program utilized in the diagnosis, checkout, and debugging of various devices in a computing system. Necessary to the use of the "FRIEND" device was the source code. IBM considered it as confidential property and it was secured carefully. The court found that one of the IBM

94. 504 F.2d 518 (5th Cir. 1974).
95. *Id.* at 529.
96. 510 F.2d 894 (10th Cir. 1975).

> employees hired by Telex took a copy of the source code with him to Telex and that Telex used this misappropriated material in order to develop a Merlin-type disk file system. The court further found that when Telex sold that project to the Control Data Corporation in May 1972, it also sold the "FRIEND" source code to Control Data for $500,000.[97]

In cases such as *Lykes* and *Telex* where the plaintiff can show that the defendant has stolen an actual source or object code, the inference is reasonably clear that the defendant has sought to utilize the "unique logic and coherence" of plaintiff's software rather than develop a competing software system through the protected use of generic or generally known skills. Unfortunately for trade secret plaintiffs, the ease of disguising software as described above makes the discovery of actual duplication or theft of source or object code very difficult. Moreover, it is often equally difficult to uncover the mechanism by which the theft occurred since software stored in a computer memory can sometimes be remotely stolen over telephone lines. In fact, most commentators agree that a knowledgeable computer specialist can, in many instances, steal software in a manner which makes detection virtually impossible.[98]

### C. Circumstantial Evidence of Time and Expense of Development Tending to Establish Misappropriation of the Trade Secrets

The protectible "competitive head start" element of software provides the key to proving most alleged software-related trade secret infringement in the absence of direct evidence of misappropriation (or the "smoking gun evidence") such as described in the preceding section. Courts have been quick to recognize that where plaintiff spends large sums of money or a great deal of time and effort to develop a specific software package and defendant, who had access to or participated in the development of such software, produces a functionally similar package in a fraction of the time or at a fraction of the cost, there is a high probability that the defendant has utilized more than generally known skills or information in the development of the competing system. This inference is particularly strong where a subsequent employer hires the plaintiff's employee for the express purpose of having him develop such a system.

Thus, in *Telex Corp. v. IBM*,[99] the court found the following evi-

97. *Id.* at 911.

98. *See* Gemignani, *supra* note 93, at 288; Roddy, *The Federal Computer Systems Protection Act*, 7 Rut. J. Computer Tech. & L. 343, 345 (1980).

99. 510 F.2d 894 (10th Cir. 1975). *See also* Extrin Foods v. Leighton, 115 N.Y.S.2d 429 (1952) (after leaving plaintiff laboratory's employ, two employees immediately be-

dence particularly significant in establishing trade secret misappropriation by Telex of IBM's software:

> In November 1970, Telex hired John K. Clemens, who had been IBM's engineering program manager for the Merlin project. Clemens was fully informed of the aspects of this program, including the development and design, manufacturing, sales and forecasts. He was hired for the purpose of developing a Merlin-type disk storage system for Telex. In addition to a substantial salary and stock options, Clemens was given a $500,000 bonus if he produced a Telex Merlin-type system for delivery to a Telex customer prior to November 30, 1972. Telex also set out to hire other key personnel in connection with IBM's Merlin project offering them high salaries, bonuses, and stock options. Telex needed to develop this in eighteen months, a schedule which the court found would have been impossible without the thefts since it had taken IBM five years to develop the project. Telex knowingly and intentionally used the IBM trade secrets and hired a number of new employees in order to bring this about. The [district] court concluded that Telex succeeded in misappropriating IBM's trade secrets and appropriating them into the Telex 6830.[100]

A former employee can, of course, always argue that he was able to develop a competing system more quickly and at less expense than its prototype by virtue of the generally known skills he either learned or refined in the development of the prototype. While this argument can plausibly explain certain cost and time efficiencies in the development of a subsequent version of software, it cannot, given the tedious process of software development, explain away substantial variations in costs and time of development. In any event, it is clearly more productive in most software related trade secret cases to have the trier of fact focus on these elements (which are not likely in many cases to produce conflicting expert testimony) rather than on conflicting expert testimony over the substantive similarities of the systems.

---

gan producing emulsion similar in chemical and physical properties to that produced by plaintiff); Space Aero Prod. Co., 208 A.2d 74 (Md.), *motion for rearg. denied*, 208 A.2d 699 (Md.), *cert. denied*, 382 U.S. 843 (1965) (plaintiff's former employees started their own corporation and within twenty-nine days of receiving corporate charter were producing oxygen breathing hose identical to that of plaintiff, despite a long history of competitors' inability to duplicate process by which plaintiff produced the hose); Ungar Tools, Inc. v. Sid Ungar Co., 192 Cal. App. 2d 398 (1961), *disapproved on other grounds*, Nichols v. Hast, 62 Cal. 2d 598 (1965) (plaintiff employee developed electric soldering tools over period of many years through substantial expenditures of time and effort; former employees of plaintiff while working for a subsequent employer developed similar product through expenditure of nominal sums and effort); Annot., 30 A.L.R.3d 631.

100. 510 F.2d at 911 (footnote omitted).

### D. Circumstantial Evidence of Error Duplication and Exact Duplication of Arbitrary Code Tending to Establish Misappropriation of Trade Secret Elements of Software

Unlike many products, software that has operated without problems for extended periods of time in a productive mode may nonetheless contain latent programming errors which have not become manifest because the system has not been called upon to perform the exact task using the exact data required to trigger the error. A trade secret plaintiff who can demonstrate that defendant's software containing allegedly misappropriated trade secret information includes latent programming errors which are also included in plaintiff's original version will have a strong case for establishing wrongful misappropriation. The evidentiary inference which arises in such a case is much the same as that which has arisen when students are accused of cheating on a multiple choice exam on the basis of making a statistically improbable number of identical mistakes. In such a case, it should be clear that defendant used specific programming decisions made in the course of developing plaintiff's system rather than independently developing a comparable system through the use of generally known skills which have merely produced functional similarity. Similar inferences arise where specific portions of defendant's system contain a code which is identical to that of plaintiff's system in an area where there are a wide variety of different programming decisions or coding protocols which could have been used to achieve substantially the same result.

In many instances, the significance of focusing on duplication of a specific error or discrete portion of a code is that such duplication can frequently be found in software that may in fact have been designed by an employee through the use of his former employer's software, but which has been disguised or revised in many respects to avoid detection of such improper design. Thus, in *Structural Dynamics Research Corp. v. Engineering Mechanics Research Corp.*,[101] the court based a finding of trade secret misappropriation by plaintiff's former employees upon the following factual findings:

> At a pretrial conference the court directed to make a copy of the static portion of the NISA code available to plaintiff's counsel and experts pursuant to a protective order. The code which was furnished was dated December, 1974, and reflected many revisions made subsequent to defendants' initial code. Defendants have represented that no prior version of the NISA code remained. Portions of the NISA code were compared to the NIESA code as it existed in January 1973. On the basis of this comparison, plaintiff's experts,

101. 401 F. Supp. 1102 (E.D. Mich. 1975).

> Dr. Anderson of the Department of Aerospace Engineering at the University of Michigan, and Michael Coble, a computer programmer also affiliated with the University, concluded that defendants must have copied from the NIESA code. They made a careful analysis of the two programs and found not only similarity in the overall structure and organization (some of which might be explainable on functional grounds) but they found identical segments of code which were solely arbitrary and, most significantly, deviations or quasi-mistakes which, in their judgment, could only be explained by copying. Victor Nicholas, who completed the development of NIESA-SUPERB at SDRC, testified that the input data cards prepared by Surana for NIESA were taken verbatim into NISA. Except for cross-examination, defendants did not address these specifics relied on by the experts, but attributed such similarities as existed to Surana's memory. The court does not accept this explanation. Memory alone cannot explain the specifics which according to the experts do not make sense but are explainable only by copying. The court finds that defendants copied from the physical NIESA code.[102]

### E. Establishing the Substantive Uniqueness of Software

Not all software must rest its claim for trade secret protection upon specific elements which give it a unique logic and coherence to differentiate it from competing software in a market filled with functionally similar products. Software is frequently developed for use in a special application so as to achieve a certain result which has not theretofore been accomplished by competing software developers. In similar circumstances in other industries, the courts have recognized that some of the skills acquired by an employee in the course of developing or receiving access to a substantively unique item would not have been acquired by the employee in the course of employment with others and therefore should not be viewed as generic to or generally known in the industry entitling it to trade secret protection.

For example, in *Plant Industries, Inc. v. Coleman*,[103] the court in applying California law found that plaintiff possessed trade secrets relating to a special method for processing citrus peels. In granting injunctive relief against plaintiff's former employee and such employee's new employer, the court specifically noted that no one other than plaintiff had obtained the results produced by plaintiff's method for processing citrus peels and therefore concluded that (i) had the defendant employee worked for another employer he would not have acquired the knowledge he now claimed the right to

102. *Id.* at 1117.

103. 287 F. Supp. 636 (C.D. Cal. 1968).

use, and that (ii) such knowledge constituted trade secrets of plaintiff rather than generally known skills, the preemption of which would unreasonably restrict the defendant employee's mobility.[104]

It seems clear that if the unique logic and coherence of two functionally similar software systems provides each of those systems with sufficient uniqueness to create a presumption of competitive advantage triggering trade secret protection, any additional uniqueness in substantive result achieved should provide a plaintiff with an even stronger case for trade secret protection. Unlike trade secret misappropriation claims related to software systems in areas where a great number of functionally similar systems exist and which may require searching for the "smoking gun," discrepancies in the development time or cost, or duplicative errors in portions of code, courts dealing with substantive uniqueness may be able to find trade secret infringement based primarily on the functional similarity of defendant's system to that of plaintiff.

### F. Detailed Comparison of Constituent Elements of Predecessor and Allegedly Infringing Software Systems

While the task of a trade secret plaintiff is certainly simplified upon discovery of the "smoking gun" or circumstantial evidence showing unreasonably small time and cost of development or duplication of arbitrary code or latent errors, such a discovery is not the only means of establishing trade secret misappropriation in a software context. The option remains for plaintiff to conduct a detailed comparison of the constituent elements of his software and the allegedly infringing software in order to establish similarities indicating misappropriation rather than independent development.

In an unpublished work, Gerald H. Larsen, formerly president of Unicorn Systems Company, a Los Angeles based software consulting company, has isolated the following constituent elements of most software which may be the focus of a trade secret plaintiff in attempting to establish the misappropriation of his software by comparison of the two systems:

---

104. *See also* Allen Mfg. Co. v. Loika, 144 A.2d 306 (Conn. 1958) (trade secret alleged in warm-heading process used in manufacture of screws; in finding in favor of plaintiff against its former employees, court noted that of plaintiff's many competitors, only one had developed similar process).

External or Functional Elements

(i) Input/Output
(ii) Data Base Flow
(iii) Manner in which system accumulates history and the scope of such generated history
(iv) Error Detection Process
(v) Particular Formulas (e.g., optimum re-order point in an inventory control system)
(vi) The unique combination of all of the foregoing in a particular system

Internal Elements

(i) Programming language and programming techniques
(ii) Functional and temporal relationships between two or more programs or transactions
(iii) Sub-program structures (i.e., breakdown of tasks into specific components)
(iv) Optimization Techniques (e.g., use of a register to hold portion of data base for repetitive functions)
(v) Tasks which logically could have been included in the system but were not
(vi) Arbitrary Limits (e.g., size of files)
(vii) The unique combination of all the foregoing in a particular system

Proof of misappropriation through comparison of the above constituent elements in two software systems relies upon the fact that, in the process of software development, the definition of a particular task does not dictate its solution. While comparably skilled systems analysts or programmers might independently arrive at comparable tasks which must be performed by functionally similar software systems and might understand the need to utilize all of the above elements to provide the software with the capability to perform such tasks, the creation of such elements can, in most circumstances, be accomplished in a large variety of forms. The specific way in which each of the above elements are utilized in a software system to accomplish a specific task is, of course, what gives the system its "unique logic and coherence."

Because of the very large number of decisions which must be made by a systems analyst or programmer in creating the constituent elements of a software system, it should be possible to establish trade secret misappropriation in a software context by reference to what Mr. Larsen has referred to as the "frequency of remarkable co-

incidences." That is, the more often the constituent elements of a software system are very similar, despite the endless variety of forms in which such elements could have appeared, the more likely it is that an act of misappropriation has occurred.

It is important to note in this context that the comparison of constituent elements will not in all circumstances be possible at the coding level. For example, the comparable use by two systems of a memory register in the performance of a particular repetitive task might be a "remarkable coincidence" tending to show misappropriation despite the fact that defendant has tried to disguise such misappropriation by coding such memory register in a manner dissimilar to that existing in plaintiff's system. While it might be argued that the use of memory registers in a design or programming technique commonly known in the software industry, the use of such a register in a particular context to achieve a particular result can be viewed as a specific design or programming decision not necessarily entailed by the functional task of the system.

The result achieved through use of the memory register could have been accomplished without such memory register by repetitive accessing of the data base, although such an alternative solution might require additional allocations of computer resources and therefore would be less economical. Since the use of memory registers is, however, a commonly known design or programming technique, comparable use of such technique in two software systems might not, in itself, establish trade secret misappropriation rather than independent development. Accordingly, a plaintiff's chances of proving misappropriation will improve in some direct proportion to the number of such similarities which appear between his software system and that of defendant.

## V. CONCLUSION

Industry observers are often quick to criticize the efficacy of trade secret protection for software. Simply stated, these critics argue that a radically new technology such as software cannot be accommodated within a legal framework which evolved prior to the development of the technology. This argument is premised on the difficulty of applying standard trade secret principles to the typical factual situation present in a case of alleged misappropriation of software. The complexity of the generic/specific issue in the context of employee-developed software is, of course, a good example of such difficulty.

As the above discussion demonstrates, the contours of trade secret law have evolved in response to conflicting public policies of major magnitude. The recent emergence of the software industry

requires that a balance between such conflicting policies be struck in a new factual environment. Courts have been able to strike such a balance in the past by adapting traditional trade secret doctrine to emerging technologies. Based on the decisions which have been handed down to date, there is good reason to believe that traditional trade secret doctrine will provide the courts with an appropriate framework within which to grapple with the difficult and far reaching economic and social issues currently presented by the data processing industry.

## APPENDIX

## CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENTS

### A. Current Employees or Current Independent Contractors

The undersigned is an employee or independent contractor working for Laser Media, Inc. ("Company"). This Agreement is intended to formalize in writing certain understandings and procedures which have been in effect since the time the undersigned was initially employed or engaged by Company. In consideration of the undersigned's original and continuing employment with or work for Company in a capacity in which he or she may receive or contribute to the production of Confidential Information (as defined below) the undersigned hereby confirms his or her understanding and agreement as follows:

1. For purposes of this Agreement, "Confidential Information" shall mean information or material proprietary to Company or designated as Confidential Information by Company and not generally known by non-Company personnel, which the undersigned develops or of which the undersigned may obtain knowledge or access through or as a result of the undersigned's relationship with Company (including information conceived, originated, discovered or developed in whole or in part by the undersigned). The Confidential Information includes, but is not limited to, the following types of information and other information of a similar nature (whether or not reduced to writing): discoveries, ideas, concepts, software in various stages of development, designs, drawings, specifications, techniques, models, data, source code, object code, documentation, diagrams, flow charts, research, development, processes, procedures, "know-how," marketing techniques and materials, marketing and development plans, customer names and other information related to customers, price lists, pricing policies and financial information. Confidential Information also includes any information described above which Company obtains from another party and which Company treats as proprietary or designates as Confidential Information, whether or not owned or developed by Company. INFORMATION PUBLICLY KNOWN THAT IS GENERALLY EMPLOYED BY THE TRADE AT OR AFTER THE TIME THE UNDERSIGNED FIRST LEARNS OF SUCH INFORMATION, OR GENERIC INFORMATION OR KNOWLEDGE WHICH THE UNDERSIGNED WOULD HAVE LEARNED IN THE COURSE OF SIMILAR EMPLOYMENT OR WORK ELSEWHERE IN THE TRADE, SHALL NOT BE DEEMED PART OF THE CONFIDENTIAL INFORMATION.

2. All notes, data, reference materials, sketches, drawings, memo-

randa, documentation and records in any way incorporating or reflecting any of the Confidential Information and all proprietary rights therein, including copyrights, shall belong exclusively to Company and the undersigned agrees to turn over all copies of such materials in the undersigned's control to Company upon request or upon termination of the undersigned's employment with Company.

3. The undersigned agrees during his employment by Company and thereafter to hold in confidence and not to directly or indirectly reveal, report, publish, disclose or transfer any of the Confidential Information to any person or entity, or utilize any of the Confidential Information for any purpose, except in the course of the undersigned's work for Company.

4. The undersigned agrees that any inventions, ideas or original works of authorship in whole or in part conceived or made by the undersigned during or after the term of his or her employment or relationship with Company which are made through the use of any of the Confidential Information or any of Company's equipment, facilities, supplies, trade secrets or time, or which relate to the Company's business or the Company's actual or demonstrably anticipated research and development, or which result from any work performed by the undersigned for Company, shall belong exclusively to Company and shall be deemed part of the Confidential Information for purposes of this Agreement whether or not fixed in a tangible medium of expression. Without limiting the foregoing, the undersigned agrees that any such original works of authorship shall be deemed to be "works made for hire" and that Company shall be deemed the author thereof under the U.S. Copyright Act (Title 17 of the U.S. Code), provided that in the event and to the extent such works are determined not to constitute "works made for hire" as a matter of law, the undersigned hereby irrevocably assigns and transfers to Company all right, title and interest in such works, including but not limited to copyrights. This agreement shall be construed in accordance with the provisions of Section 2870 of the California Labor Code relating to inventions made by an employee, and accordingly this agreement is not intended and shall not be interpreted to assign to or vest in Company any of the undersigned's rights in any inventions other than those described in the first sentence of this Paragraph 4.

5. Because of the unique nature of the Confidential Information, the undersigned understands and agrees that Company will suffer irreparable harm in the event that the undersigned fails to comply with any of his or her obligations under Sections 2, 3 or 4 above and that monetary damages will be inadequate to compensate Company for such breach. Accordingly, the undersigned agrees that Company

will, in addition to any other remedies available to it at law or in equity, be entitled to injunctive relief to enforce the terms of Sections 2, 3 and 4 above.

6. This Agreement shall be governed by California law applicable to contracts between residents of California which are wholly executed and performed in California. This Agreement contains the full and complete understanding of the parties with respect to the subject matter hereof and supersedes all prior representations and understandings, whether oral or written. In the event that any provision hereof or any obligation or grant of rights by the undersigned hereunder is found invalid or unenforceable pursuant to judicial decree or decision, any such provision, obligation or grant of rights shall be deemed and construed to extend only to the maximum permitted by law, and the remainder of this Agreement shall remain valid and enforceable according to its terms.

I agree to the above terms and acknowledge receipt of a copy of this Agreement.

Date: _____

Signature: _____

Name (printed): _____

Social Security No: _____

Mailing Address: _____

B. NEW EMPLOYEES OR NEW INDEPENDENT CONTRACTORS

The undersigned is being hired to perform services as an employee or independent contractor working for Laser Media, Inc. ("Company"). In consideration of the undersigned's original and continuing employment with or work for Company in a capacity in which he or she may receive access or contribute to the production of Confidential Information (as defined below), the undersigned agrees as follows:

1. For purposes of this Agreement, "Confidential Information" shall mean information or material proprietary to Company or designated as Confidential Information by Company and not generally known by non-Company personnel, which the undersigned develops or of which the undersigned may obtain knowledge or access through or as result of the undersigned's relationship with Company (including information conceived, originated, discovered or developed in whole or in part by the undersigned). The Confidential Information includes, but is not limited to, the following types of information and other information of a similar nature (whether or not reduced to writing): discoveries, ideas, concepts, software in various stages of development, designs, drawings, specifications, techniques, models, data, source code, object code, documentation, diagrams, flow charts, research, development, processes, procedures, "know-how," marketing techniques and materials, marketing and development plans, customer names and other information related to customers, price lists, pricing policies and financial information. Confidential Information also includes any information described above which Company obtains from another party and which Company treats as proprietary or designates as Confidential Information, whether or not owned or developed by Company. INFORMATION PUBLICLY KNOWN THAT IS GENERALLY EMPLOYED BY THE TRADE AT OR AFTER THE TIME THE UNDERSIGNED FIRST LEARNS OF SUCH INFORMATION, OR GENERIC INFORMATION OR KNOWLEDGE WHICH THE UNDERSIGNED WOULD HAVE LEARNED IN THE COURSE OF SIMILAR EMPLOYMENT OR WORK ELSEWHERE IN THE TRADE, SHALL NOT BE DEEMED PART OF THE CONFIDENTIAL INFORMATION.

2. All notes, data, reference, materials, sketches, drawings, memoranda, documentation and records in any way incorporating or reflecting any of the Confidential Information and all proprietary rights therein, including copyrights, shall belong exclusively to Company and the undersigned agrees to turn over all copies of such materials in the undersigned's control to Company upon request or upon termination of the undersigned's employment with Company.

3. The undersigned agrees during his employment by Company

and thereafter to hold in confidence and not to directly or indirectly reveal, report, publish, disclose or transfer any of the Confidential Information to any person or entity, or utilize any of the Confidential Information for any purpose, except in the course of the undersigned's work for Company.

4. The undersigned agrees that any inventions, ideas or original works of authorship in whole or in part conceived or made by the undersigned during or after the term of his or her employment or relationship with Company which are made through the use of any of the Confidential Information or any of Company's equipment, facilities, supplies, trade secrets or time, or which relate to the Company's business or the Company's actual or demonstrably anticipated research and development, or which result from any work performed by the undersigned for Company, shall belong exclusively to Company and shall be deemed part of the Confidential Information for purposes of this Agreement whether or not fixed in a tangible medium of expression. Without limiting the foregoing, the undersigned agrees that any such original works of authorship shall be deemed to be "works made for hire" and that Company shall be deemed the author thereof under the U.S. Copyright Act (Title 17 of the U.S. Code), provided that in the event and to the extent such works are determined not to constitute "works made for hire" as a matter of law, the undersigned hereby irrevocably assigns and transfers to Company all right, title and interest in such works, including but not limited to copyrights. This agreement shall be construed in accordance with the provisions of Section 2870 of the California Labor Code relating to inventions made by an employee, and accordingly this agreement is not intended and shall not be interpreted to assign to or vest in Company any of the undersigned's rights in any inventions other than those described in the first sentence of this Paragraph 4.

5. Because of the unique nature of the Confidential Information, the undersigned understands and agrees that Company will suffer irreparable harm in the event that the undersigned fails to comply with any of his or her obligations under Sections 2, 3 or 4 above and that monetary damages will be inadequate to compenstate Company for such breach. Accordingly, the undersigned agrees that Company will, in addition to any other remedies available to it at law or in equity, be entitled to injunctive relief to enforce the terms of Sections 2, 3 and 4 above.

6. This Agreement shall be governed by California law applicable to contracts between residents of California which are wholly executed and performed in California. This Agreement contains the full and complete understanding of the parties with respect to the sub-

ject matter hereof and supersedes all prior representations and understandings, whether oral or written. In the event that any provision hereof or any obligation or grant of rights by the undersigned hereunder is found invalid or unenforceable pursuant to judicial decree or decision, any such provision, obligation or grant of rights shall be deemed and construed to extend only to the maximum permitted by law, and the remainder of this Agreement shall remain valid and enforceable according to its terms.

I agree to the above terms and acknowledge receipt of a copy of this Agreement.

Date: _____

Signature: _____

Name (printed): _____

Social Security No: _____

Mailing Address: _____

C. VISITORS

It is contemplated that the undersigned may from time to time be admitted to the premises of Laser Media, Inc. ("Co."). In consideration of the undersigned's access to the premises of Company in a capacity in which he or she may receive or obtain knowledge of Confidential Information (as defined below), the undersigned, hereby confirms his or her understanding and agreement as follows:

1. For purposes of this Agreement, "Confidential Information" shall mean information or material proprietary to Company or designated as Confidential Information by Company and not generally known by non-Company personnel, of or to which the undersigned may obtain knowledge or access through or as a result of the undersigned's relationship with Company or access to Company's premises. The Confidential Information includes, but is not limited to, the following types of information and other information of a similar nature (whether or not reduced to writing): discoveries, ideas, concepts, software in various stages of development, designs, drawings, specifications, techniques, models, data, source code, object code, documentation, diagrams, flow charts, research, development, processes, procedures, "know-how," marketing techniques and materials, marketing and development plans, customer names and other information related to customers, price lists, pricing policies and financial information. Confidential Information also includes any information described above which Company obtains or has obtained from another party and which Company treats as proprietary or designates as Confidential Information, whether or not owned or developed by Company.

2. The undersigned agrees not to remove from Company's premises or to reproduce any notes, data, reference materials, sketches, drawings, memoranda, documentation or records.

3. The undersigned agrees to hold in confidence and not to directly or indirectly reveal, report, public, disclose or transfer any of the Confidential Information to any person or entity, or utilize any of the Confidential Information for any purpose at any time.

4. Because of the unique nature of the Confidential Information, the undersigned understands and agrees that Company will suffer irreparable harm in the event that the undersigned fails to comply with any of his or her obligations under Sections 2 or 3 above and that monetary damages will be inadequate to compensate Company for such breach. Accordingly, the undersigned agrees that Company will, in addition to any other remedies available to it at law or in equity, be entitled to injunctive relief to enforce the terms of Sections 2 and 3.

5. This Agreement shall be governed by California law applicable to contracts between residents of California wholly executed and performed in California. This Agreement contains the full and complete understanding of the parties with respect to the subject matter hereof and supersedes all prior representations and understandings, whether oral or written.

I agree to the above terms and acknowledge receipt of a copy of this Agreement.

Date: _____

Signature: _____

Name (printed): _____

Social Security No: _____

Mailing Address: _____